NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NEW TECHNOLOGIES AND EMERGING THREATS: PERSONNEL SECURITY ADJUDICATIVE GUIDELINES IN THE AGE OF SOCIAL NETWORKING

by

James P. Festa

December 2012

Thesis Advisor:	Robert Josefek
Second Reader:	Samantha Smith-Pritchard

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE NEW TECHNOLOGIES AND EMERGING THREATS: PERSONNEL SECURITY ADJUDICATIVE GUIDELINES IN THE AGE OF SOCIAL NETWORKING		**5. FUNDING NUMBERS**	
6. AUTHOR(S) James P. Festa			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Publicized incidents involving espionage or violence by government employees with security clearances have raised concern for the personnel security community. The guidelines used to adjudicate security clearances were last updated in 2005; since that time, significant technological developments, especially in social media and communications, have emerged.

This thesis developed a comprehensive list of current Internet behaviors, and used the list to examine Internet behavior in cases of cleared government employees who have been charged with espionage or terrorism-related crimes since 2008. Cases showed a trend of increasing variety of behaviors in these cases with time. In contrast, data from the Defense Office of Hearings and Appeals (DOHA) pertaining to proposed security clearance denials related to the Use of Information Technology Systems guideline showed a slight decrease. Incorporation of cybervetting into the background investigation process is proposed as a measure to enhance mitigation of questionable Internet behaviors, and may result in an increase in security clearance denials.

Examination of the list of Internet behaviors against the current adjudicative guidelines resulted in recommended improvements for the Foreign Influence, Financial Considerations, Personal Conduct, Handling Protected Information, and Use of Information Technology Systems guidelines. Operations Security is proposed as a completely new adjudicative guideline.

14. SUBJECT TERMS Personnel security; adjudicative guidelines; security clearance; government employment; suitability; background investigation; cybervetting; computers; social media; social networking; insider threat; espionage; terrorism; hacking; Internet crime; cyber bullying; doxing; phishing; operations security (OPSEC); Defense Office of Hearings and Appeals (DOHA); Guideline M; Use of Information Technology Systems; online gaming; virtual worlds			**15. NUMBER OF PAGES** 103 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NEW TECHNOLOGIES AND EMERGING THREATS: PERSONNEL SECURITY ADJUDICATIVE GUIDELINES IN THE AGE OF SOCIAL NETWORKING

James P. Festa
Supervisory Personnel Security Specialist, U.S. Citizenship and Immigration Services,
Department of Homeland Security
B.A., University of New Hampshire, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2012

Author: James P. Festa

Approved by: Robert Josefek
Thesis Advisor

Samantha Smith-Pritchard
Second Reader

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Publicized incidents involving espionage or violence by government employees with security clearances have raised concern for the personnel security community. The guidelines used to adjudicate security clearances were last updated in 2005; since that time, significant technological developments, especially in social media and communications, have emerged.

This thesis developed a comprehensive list of current Internet behaviors, and used the list to examine Internet behavior in cases of cleared government employees who have been charged with espionage or terrorism-related crimes since 2008. Cases showed a trend of increasing variety of behaviors in these cases with time. In contrast, data from the Defense Office of Hearings and Appeals (DOHA) pertaining to proposed security clearance denials related to the Use of Information Technology Systems guideline showed a slight decrease. Incorporation of cybervetting into the background investigation process is proposed as a measure to enhance mitigation of questionable Internet behaviors, and may result in an increase in security clearance denials.

Examination of the list of Internet behaviors against the current adjudicative guidelines resulted in recommended improvements for the Foreign Influence, Financial Considerations, Personal Conduct, Handling Protected Information, and Use of Information Technology Systems guidelines. Operations Security is proposed as a completely new adjudicative guideline.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADAMS	Anomaly Detection at Multiple Scales
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CINDER	Cyber Insider Threat
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DoD	Department of Defense
DOHA	Defense Office of Hearings and Appeals
DSCA	Defense Security Cooperation Agency
FBI	Federal Bureau of Investigation
FSI	United States Department of State, Foreign Service Institute
HR	Human Resources
ICPG	Intelligence Community Policy Guidance
INR	United Stated Department of State, Bureau of Intelligence and Research
IP	Internet Protocol
IT	Information Technology
ODNI	Office of the Director of National Intelligence
OPM	United States Office of Personnel Management
OPSEC	Operations Security
PERSEREC	Defense Personnel Security Research Center
PRC	People’s Republic of China
SCI	Sensitive Compartmented Information

SSL	Secure Socket Layer
U.S.	United States
VoIP	Voice Over Internet Protocol

ACKNOWLEDGMENTS

I would like to thank the faculty and staff of the Center for Homeland Defense and Security at the Naval Postgraduate School for their professionalism, dedication, and support. Additionally, I would like to thank the staff of the Defense Personnel Security Research Center for their generosity of time, expertise, and perspective in the area of personnel security research.

Special thanks to Drs. Josefek and Smith-Pritchard, for their time, energy, expertise, cooperative spirit, and motivational support. I could not have asked for a better team.

I would also like to thank the Department of Homeland Security for having the vision to establish, fund, and support the Center; the U.S. Citizenship and Immigration Services for their encouragement to participate; and my supervisors and coworkers in the Personnel Security Division who supported my attendance in the program and my time away from the office. I am hopeful that this thesis, as well as my future professional contributions, may one day generate a return on your investment in me.

Most of all, I thank my family who supported me, sacrificed for me, and put up with me throughout the duration of my attendance. This was a team effort on many levels, and I am forever grateful to all of you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. NEW TECHNOLOGIES AND EMERGING THREATS: PERSONNEL SECURITY ADJUDICATIVE GUIDELINES IN THE AGE OF SOCIAL NETWORKING

A. INTRODUCTION

Recent events have shown that the U.S. government's information, personnel, and facilities are vulnerable to insider threats. Army Major Nidal Hasan is charged with opening fire at Fort Hood on November 5, 2009, killing 13 people and wounding 32 more.[1] Six months later, Bradley Manning was arrested for his alleged involvement in the public disclosure of over 250,000 classified documents.[2] Both individuals held active security clearances. One of the ways the government works to reduce the risk posed in such cases is to conduct background investigations on individuals seeking access to classified national security information. These background investigations are adjudicated according to a set of guidelines known as the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information. Originally approved in 1997 and updated in 2005, they provide agencies with a framework for approving or denying access to classified information. Since 2005, society has seen advancement in technology, especially in the area of social media. However, the guidelines have not been updated to address these advancements or their implications for security clearance eligibility. In support of that objective, this thesis will examine some of the issues surrounding the integration of recent and emerging technologies into the adjudicative guidelines.

B. PROBLEM SPACE

One of the key vulnerabilities in the homeland security environment is risk posed by insider threats. Personnel security, including the investigation and adjudication of employee backgrounds, is one of a variety of disciplines that work collectively to mitigate this risk. Applicants for employment and security clearances voluntarily submit

---

[1] U.S. Senate, Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, February 3, 2011, http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2.

[2] Kevin Poulsen and Kim Zetter, "U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe," *Wired*, June 6, 2010, http://www.wired.com/threatlevel/2010/06/leak/.

to background investigations by the government, which are in turn adjudicated according to an established set of adjudicative guidelines. These guidelines were most recently updated in 2005, prior to the advent of widely popular social networking sites such as Facebook and Twitter.

The thesis examines the adjudicative guidelines in light of new developments in technology and the corresponding uses of that technology by individuals and groups. Unlike the Internet of the 1990s, today's Internet (often dubbed "Web 2.0") is more dynamic, interactive, collaborative, and user-generated. An expansive variety of platforms exist for social interaction, the sharing of media, and connecting with others from around the world in ways that were never before possible. While enabling collaborative efforts for noble causes such as responding to natural disasters, fighting disease, and raising money for charity, these Internet platforms have also provided new ways to further criminal, illicit, or otherwise questionable behaviors that could impact eligibility for a security clearance or employment suitability. This thesis seeks to further our understanding of what kinds of activities are related to these technologies, how these technologies are used by insider threats, how the government is responding, and the impacts on the personnel security guidelines. This topic is important to investigate because a government's policies should advance alongside the society it intends to serve. If policies become outdated, there could be the potential for increased government vulnerability as new technology would allow for potentially dangerous practices and behaviors that were not considered at the time the policies were created.

This research effort focuses on the adjudicative guidelines that accompany Executive Order 12968, which were most recently updated and approved in 2005.[3] A different standard, Intelligence Community Policy Guidance (ICPG) 704.2, is used for

[3] Katherine Herbig, *The Evolution of Adjudicative Guidelines in the Department of Defense* (Monterey, CA: Department of Defense Personnel Security Research Center, 2011), 26, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA563952.

adjudicating access to Sensitive Compartmented Information (SCI).[4] While this thesis will not explicitly evaluate ICPG 704.2, its implications could also inform discussion of possible updates to that standard as well.

C. RESEARCH QUESTIONS

1. In what kinds of online activities are insider threats engaging?

2. How is online activity by insider threats changing over time?

3. What impacts do emerging information technologies have on the capabilities and limitations of the personnel security adjudicative guidelines to mitigate insider threats?

4. Further, how can the adjudicative guidelines address such impacts and provide federal government agencies with the necessary tools to mitigate this risk?

[4] Herbig, *The Evolution of Adjudicative Guidelines*, 32.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

This literature review examines the existing research on the topic of insider threat in general, as well as the topic of current technology's impact on personnel security guidelines. This review found four main approaches to understanding insider threat in the literature: demographical, psychological, environmental, and meta-analytical. There were few resources that examined the ways in which information technology can be used as a tool in support of these four approaches, suggesting an opportunity for further research in related areas.

It is important to identify a working definition of two key terms used in this thesis. A RAND Corporation report defines the insider as "Anyone with access, privilege, or knowledge of information systems and services."[5] This definition focuses on information systems, but for the purpose of this thesis, an insider will include any person with special access, clearance, privilege, or knowledge of information exceeding that of the general public, not limited to information systems alone. This includes all federal agency employees, security clearance holders, authorized contractors, detailees, student interns, or other individuals given such privileges. The same RAND report defines a "malicious insider" as an insider who is "motivated to intentionally adversely impact an organization's mission."[6] This thesis will combine these two concepts into one definition of insider threat: Any person with access, clearance, knowledge of information, or other privilege exceeding that of the general public, who is motivated to intentionally adversely impact an organization's mission.

The other key term used in this thesis is espionage. As this is a more common term and concept than insider threat, a simple Merriam-Webster dictionary definition will suffice as a starting point: "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing

---

[5] Richard C. Brackney and Robert H. Anderson, *Understanding the Insider Threat: Proceedings of a March 2004 Workshop* (Santa Monica, CA: RAND Corporation, 2004), 10, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf.

[6] Ibid.

company." This definition implies that the information provides some sort of advantage for the collector in an environment of competition, such as for one government or business over another. It also implies that the information is not already available through overt means, such as publicly available sources. The definition also appears to be limited to human collection methods and does not include use of technical or automated means of obtaining information. In light of these observations and for the purpose of this thesis, espionage will be defined as the practice of obtaining secret, non-public, or otherwise-privileged information about a competitor. Espionage, by this definition, would be largely engaged in by governments and businesses, but not limited to these entities. Terrorists, criminals, and members of the general public could also engage in this activity insofar as it may further their various individual aims. Thus the nexus between insider threat and espionage is that espionage is one of the activities that malicious insiders may engage in, and insider threat is the overall term to describe this dynamic.

With these two key terms in mind, the key research on insider threat can be examined more fully. As described initially, the relevant literature can generally be organized into four main approaches to the understanding of insider threat. These approaches can be construed as lenses through which to understand the insider threat dynamic and to find ways to prevent or mitigate its negative impacts. The following three sections describe these approaches and briefly discuss the implications, advantages, and disadvantages of each.

A. DEMOGRAPHICAL APPROACH

This approach studies the demographics of past insider threat actors in order to identify common traits or characteristics. Some of the research efforts undertaken by the Department of Defense (DoD) Personnel Security Research Center (PERSEREC) have included statistical analysis of demographic information in past offenders of espionage, a form of insider threat activity. Examples of such demographic information include country of origin, citizenship status, age, gender, religion, and other factors. Researchers using this approach can then draw statistical conclusions to characterize and understand commonalities across different offenders. For example, PERSEREC has created a

database that captures biographical and employment characteristic data from published espionage cases, which can then be analyzed to draw statistical conclusions to guide policy and decision making. One study of this database found that since the end of the Cold War, individuals who engage in espionage are statistically more likely to be male, non-white, over the age of 30, married, well-educated, heterosexual, not in the uniformed military, and hold a security clearance.[7] While explicitly not an attempt to create a single profile of a spy[8], readers can draw profile-like conclusions in specific aspects of a demographic. Notably, this is also the approach taken by researchers, including renowned terrorism expert Bruce Hoffman, in a 1990 study of insider crime at nuclear facilities.[9] The obvious downside of this approach is that it is not fully predictive, as there may be individuals who commit insider threat activities but do not fit the statistical profile. Decision makers who allocate resources according to a statistical profile may still fail to identify or prevent an insider from causing damage.

B. PSYCHOLOGICAL AND ENVIRONMENTAL APPROACHES

Another approach to studying insider threat is to study the psychological characteristics and traits of individuals, in order to identify individuals with problematic or abnormal psychological conditions that could indicate propensity toward insider threat activity. A key research item, "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider" was published in 1998 by Eric Shaw, Keven Ruby, and Jerrold Post.[10] The conclusions appear to have driven, or at least are consistent with, a significant portion of the overall body of research on insider threat. The authors

---

7 Katherine L. Herbig, *Changes in Espionage by Americans, 1947-2007* (Monterrey, CA: Department of Defense Personnel Security Research Center, 2008), 7–29, http://www.dhra.mil/perserec/reports/tr08-05.pdf.

8 Katherine L. Herbig and Martin F. Wiskoff, *Espionage Against the United States by American Citizens, 1947-2001* (Monterrey, CA: Department of Defense Personnel Security Research Center, 2002), 15, http://www.dhra.mil/perserec/reports/tr02-05.pdf.

9 Bruce Hoffman, et al., *Insider Crime: The Threat to Nuclear Facilities and Programs* (Santa Monica, CA: RAND Corporation, 1990), http://www.rand.org/content/dam/rand/pubs/reports/2007/R3782.pdf.

10 Eric D. Shaw, Keven G. Ruby, and Jerrold M. Post, *The Insider Threat to Information Systems: The Psychology of the Dangerous Insider* (Richmond, VA: Department of Defense Security Institute, 1998), http://www.pol-psych.com/sab.pdf.

approach the problem as one of psychological predispositions in individuals who commit insider threat activities. They develop a psychological profile of the malicious information technology insider, which includes introversion, social and personal frustrations, computer dependency, ethical flexibility, reduced loyalty, sense of entitlement, anger at employers, and lack of empathy. The authors also caution that,

> The presence of any or all of these personal and cultural vulnerabilities does not, however, a perpetrator make. Indeed, it is more often the dynamic interaction between… personal psychology (including the vulnerabilities enumerated above) and the organizational and personal environment that leads the vulnerable [insider] down a slippery slope, at the end of which an act of information system aggression occurs.[11]

The article identifies a common pathway to insider threat: predisposing personal traits, an acute situational stressor, emotional fallout, biased decision-making or judgment failures, and failure of peers and supervisors to intervene effectively.

The approach taken by the above article can be further broken down into two components: the psychological approach as described, and an environmental approach that places psychological traits in external context. This environmental approach studies the external elements of an insider's environment that either allow or disallow him to conduct harmful activities. The focus here is on internal controls, need-to-know, password protection and encryption, the two-man rule, and other controls. In another PERSEREC report, *Insider Risk Evaluation and Audit*, the authors use analysis of past known cases of insider damage to develop self-assessments for organizations and recommended countermeasures.[12] This approach does not readily address psychological factors of employees or suggest various forms of psychological counseling to address issues. Rather, the report gives employers guidance on how to create and maintain a secure environment with internal controls. While the psychological and environmental approaches are very closely linked, it may be helpful for the insider threat analyst to break down a single set of activity into psychological and environmental components.

---

11 Shaw, Ruby, and Post, *The Insider Threat*, 8.

12 Eric D. Shaw, Lynn F. Fischer, and Andree E Rose, *Insider Risk Evaluation and Audit* (Monterrey, CA: Department of Defense Personnel Security Research Center, 2009), http://www.dhra.mil/perserec/reports/tr09-02.pdf.

C. META-ANALYTICAL APPROACH

Advances in computer technology and the automated processing of large volumes of data have enabled the development of the meta-analytical approach to identifying insider threat. The approach relies on the collection of a wide variety of employee-related data streams, including emails, phone call records, attendance including absences and leave requests, arrival and departure records, disciplinary records, computer logs, etc. Computer systems could be designed to observe this "big data" of employee behavior over time in order to build a baseline of normalcy. This baseline could then be compared to a specific individual's activities in order to identify those that are unusual for a certain job type, or new behaviors not typical of a given employee's past behavioral history. The primary challenges in this approach are that these data sources are often unavailable to federal government employers, and that such information is collected and managed in separate agency compartments such as IT, HR, Security, Contracting, or other offices and not centrally stored or analyzed in one place. These challenges would need to be addressed in order to maximize the potential of the meta-analytical approach.

Even in light of potential challenges in its application, this approach appears to be receiving the most attention in future research projects and funding. In November 2011, the Defense Advanced Research Projects Agency (DARPA) began funding a collective effort by the Georgia Institute of Technology and four other organizations to create a suite of algorithms that turn disparate data feeds into real-time alerts of anomalous activity. DARPA is funding the project for $9 million dollars under its Anomaly Detection at Multiple Scales (ADAMS) project.[13] DARPA is also funding future research on a Cyber Insider Threat (CINDER) program, with specific projects yet to be announced. This effort is seen as updating Cold War security practices for the Information Age. According to the chief security officer of RSA, Inc., "If you think classically, how would you find indicators in people's activities? Large deposits in their bank accounts, changes in the way they drive to work. Those types of human intelligence

[13] Abby Robinson, "Georgia Tech Helps to Develop a System that will Detect Insider Threats from Massive Data Sets," Georgia Institute of Technology, November 10, 2011, http://www.gatech.edu/newsroom/release.html?nid=72599.

observations that we saw classically during the Cold War, we are just extending to the dark side of cyberspace."[14] While current research articles and publications do not use meta-analysis, future research will likely provide the security community with new insights gained from such an approach.

D. APPLICATION OF PERSONNEL SECURITY POLICIES TO EMERGING TECHNOLOGIES

This review found very few reliable resources that examined ways for agencies or companies to adjudicate or otherwise justly dispose of emerging technology-based behaviors and incidents in applicant and employee backgrounds. DoD PERSEREC has published two reports that examine the practice of using online technology including social media as part of the background investigative process, which is known as cybervetting.[15] These reports provide a foundation for agencies that are examining whether or not to conduct cybervetting on their applicants, and how to do so with respect to privacy and legal constraints. These reports do not include recommendations for adjudicating the information that could be found using cybervetting techniques, perhaps because there are a variety of agencies operating at multiple levels of government including federal, tribal, state, and local, each with their own legal frameworks within which they adjudicate the collected cyber and other background information. Thus the adjudicative aspect of this topic is too agency-specific for one product to address.

Another PERSEREC project is aimed at understanding the impact of participation in cyber activities, known as cyber culture, on personnel security and more closely addresses issues related to adjudication for security clearances. One study, "Ethnographic Analysis of Second Life," examined the Second Life virtual world its impact on employment for a sample of its users. The study's goals were to: describe behaviors of

---

[14] Robert Lemos, "Analyzing Data to Pinpoint Rogue Insiders," *Dark Reading.* November 29, 2011, http://www.darkreading.com/insider-threat/167801100/security/security-management/232200401/analyzing-data-to-pinpoint-rogue-insiders.html.

[15] See Andree G. Rose, et al., *Developing a Cybervetting Strategy for Law Enforcement*, (Monterey, CA: International Association of Chiefs of Police and Defense Personnel Research Center, 2011), http://www.iacpsocialmedia.org/Portals/1/documents/CybervettingReport.pdf; and Rose, A.G. et al., *Guidance for Developing a Cybervetting Strategy for National Security Positions*, (Monterey, CA: Defense Personnel Security Research Center, 2011), (For Official Use Only).

personnel security concern that individuals exhibit in Second Life using the Adjudicative Guidelines for Determining the Eligibility for Access to Classified Information as a framework; describe the nature, breadth, and severity of real-life behavioral consequences, i.e., "spillover," resulting from involvement in Second Life; and develop an initial typology framework for distinguishing between innocuous and problematic forms of participation in Second Life.[16] This report represents the first effort identified in this literature review that explicitly tries to identify virtual behaviors of concern through the lens of the personnel security guidelines. Another related project that is under development by PERSEREC includes surveys of clearance holders to identify how they use Internet technology in order to determine how prevalent certain behaviors are in the cleared workforce.[17]

In addition to the above PERSEREC efforts, a study sponsored by the Office of the Director of National Intelligence (ODNI) surveyed the prevalence of social networking accounts in a voluntary sample of 349 security clearance holders, and then examined those social networking accounts for examples of derogatory information. The study found that Internet research yielded derogatory information on 13% of the participants, and 13% of that information was considered "possible illegal activity."[18] A key conclusion of the report was that reviewing an applicant's public online profile may allow for a more complete overview of his or her background.[19] This report was valuable in that it provided insight into the prevalence of use and derogatory information that cybervetting could yield. However, it did not describe the range of activities it counted as derogatory, and does not make recommendations regarding if or how to change the present adjudicative guidelines.

---

16 Olga Shechter, Eric Lang, and Christina Keibler, *Cyberculture and Personnel Security: Report II – Ethnographic Analysis of Second Life* (Monterey, CA: Defense Personnel Security Research Center, 2011), vii, http://www.dhra.mil/perserec/reports/tr11-03.pdf.

17 Informal conversations with PERSEREC staff, April 2012.

18 Office of the Director of National Intelligence, "Social Networking Study," In Electronic Freedom Foundation, May 14, 2010, 37, 43, https://www.eff.org/file/31845#page/1/mode/1up.

19 Office of the Director of National Intelligence, "Social Networking Study," 44.

Another study developed a taxonomy, or list, of cyber behaviors, identified prevalence rates of these behaviors in samples of two different populations, and discussed issues surrounding the prediction of cyber risk.[20] One of the report's suggestions for future research included a review of the adjudicative guidelines in light of these cyber behaviors,[21] which is consistent with the research goals of this thesis.

E. SHORTCOMINGS AND GAPS

The analysis of past and ongoing efforts shows a number of areas where the overall body of research on insider threat and cyber behaviors is potentially biased, insufficient, or lacking. The preponderance of the research has been funded and/or directed by DoD, with some efforts recently sponsored by ODNI. This fact has the potential to skew research topics or findings toward particular sets of agency needs, and may mean that not all potential approaches or aspects of insider threat have received appropriate research attention for other stakeholders, such as the homeland security community, government industry, or the not-for-profit sector. For example, the use of temporary or volunteer staff may be more widely used in other sectors and provide different challenges to vetting cyber behaviors that are not as prevalent in the defense or intelligence communities.

The other primary shortcoming in the research on insider threat is its domination by demographical and psychological approaches. While the demographical approach paints a statistical profile of past offenders, it does not show causality between demography and insider threat. The psychological approach is also incomplete, as even with all psychological indicators present a person might still not become an insider threat;[22] likewise, a person may be an insider threat without displaying any of the identified indicators. The meta-analytical approach has similar limitations in that a person's unusual patterns of activity may not necessarily mean they pose a threat. The psychological and meta-analytical approaches also have limitations on their use in the

20 Steven S. Russel, et al., *Cyber Behavior and Personnel Security: Final Report* (Minneapolis: Personnel Decisions Research Institutes, Inc., 2009), 1.

21 Ibid., 115.

22 Shaw, Ruby, and Post, *The Insider Threat to Information Systems*, 8.

government setting: many federal agencies do not conduct psychological assessments of candidates, even for security clearance positions; and the technical and privacy challenges of collecting wide-ranging data on employees may be difficult for federal agencies to overcome. Both approaches also carry significant monetary and resource costs to implement.

As for the recent efforts to understand emerging technology and impact on the security guidelines, the work has centered on taking samples of current security clearance holders, and through surveys and voluntary review of online presence, determine how these individuals use the technology. These efforts have not included more in-depth studies of actual insiders who have damaged national security to examine their online presence and activities. They have also not examined recent data on security clearance decisions to understand whether the number of cases of computer-related security clearance denials could show an increase in computer or online presence in the applicant population. Lastly, the research does not compare online behaviors with the present adjudicative guidelines to identify areas that could be improved.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHOD

As discussed in the first chapter, this thesis has four essential research questions. The first question asks in what kinds of online activities insider threats are engaging. To answer this question, a sample of case studies will be examined with special emphasis on what online or virtual activities the suspects were engaged in prior to their arrest. The case studies include federal government employees who were arrested for crimes related to espionage or terrorism. These employees all held active or previously-active security clearances at the time of arrest. Given the recent nature of the technological and social media developments, the case studies are taken only from the past five years and include individuals arrested during that time period. Online searches were conducted in order to collect relevant case information, which was used to formulate a brief case narrative and identification of online activities in which insiders were engaged.

The second research question asks how the online activity of insider threats has changed over time, including how many different activities were present for each case. To answer this question, two research activities were conducted. First, Internet and academic research[23] was conducted to develop a list of online behaviors and activities, organized by category and theme. This list was meant to be as inclusive as possible, but not exhaustive. The insider threat case studies were then analyzed for the presence of these behaviors in each case, and a numerical tally of the number of activities for each case was then conducted. This tally was designed to show, with a very limited sample, whether Internet use among the recent cases had changed, and if so, how. An increase in the number of different activities was expected, as society in general is increasing its variety of online activities and presence. The time period examined was approximately the past five years, including any case from 2008 to the present. The Case Studies section will identify these cases and provide a brief overview of each of them, which will aid in

[23] Among the sources reviewed in developing this list were Yvonne Jewkes and Majid Yar, *Handbook of Internet Crime* (Cullompton: Willan Publishing., 2010); Steven S. Russel, et. al., *Cyber Behavior and Personnel Security: Final Report*; Ken Dunham and Jim Melnick, *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet* (Boca Raton: Auerbach Publications, 2008); and *A Complete Hacker's Handbook: Everything You Need to Know About Hacking in the Age of the Web*, 1st Edition, http://www.telefonica.net/web2/vailankanni/HHB/index.html.

further discussions in later chapters. The list of cases examined there represents some of the most significant cases made public since 2008, based on damage or potential damage to the government. It is not meant to be exhaustive, but a sample of some of the most publicized cases.

The second research activity conducted to answer the question of how online activity by insider threats has changed over time was to review public data of security clearance decision appeals from the Defense Office of Hearings and Appeals (DOHA). DOHA publishes case summaries for all industrial (contractor) security clearance appeals, [24] which are the result of negative security clearance decisions by the various Department of Defense (DoD) components as well as 20 other federal departments and agencies.[25] Therefore this data represents the security clearance cases that were originally denied, whether they were overturned on appeal or not. While limited in scope to industrial security clearance appellants, it is the only public resource that shows the results of agency security clearance determinations, and provides a snapshot of at least one group of federal departments' clearance adjudication efforts. This data was analyzed to identify how many cases were based on the adjudicative guideline that addresses the use of information technology systems. The same five year period was selected as for the insider threat case studies, with 2012 numerical data collected as of October 1 and projected for the rest of the year for the purpose of this research. By doing this, this thesis sought to identify whether the government was seeing an increase, decrease, or no change in the number of security clearances it was denying based on computer misuse. An increase was expected as these security clearance applicants would logically come from the general population which is increasing its use of computers and the Internet. This expectation is based on an assumption that the ratio of IT use to misuse is essentially constant.

The third research question asks what impacts emerging technologies have on the ability of the adjudicative guidelines to mitigate insider threat. To answer this question,

[24] Defense Office of Hearings and Appeals, "Industrial Security Clearance Decisions," http://www.dod.mil/dodgc/doha/industrial/ (Accessed October 29, 2012).

[25] Defense Office of Hearings and Appeals, "Defense Office of Hearings and Appeals," http://www.dod.mil/dodgc/doha/ (Accessed October 29, 2012).

the list of online behaviors was compared with the most recent version of the adjudicative guidelines. For each online behavior, the guidelines were reviewed to identify what guideline and disqualifying paragraph could apply. The guideline paragraph number was recorded for any behaviors that could be addressed by an adjudicative guideline. If more than one guideline could apply, multiple paragraph numbers were recorded. This exercise was completed for all behaviors on the list, and it identified those online behaviors that were covered by the adjudicative guidelines and those that were not. Appendix B includes this information in detail, as well as which of the insider threat cases are publicly reported to have engaged in each behavior. This thesis then discusses these uncovered behaviors and potential instances where they could be damaging to the government, display poor judgment, or indicate an inability to safeguard sensitive information.

The fourth research question asks how the adjudicative guidelines can address the impacts of insider threats and provide agencies with the tools to do so. To answer this question, this thesis started with the behaviors that met the two criteria identified above in the third research question, i.e. those behaviors that were identified as not covered by the present adjudicative guidelines and that could reasonably case damage or indicate a potential for future damage. Such behaviors may suggest more research and consideration by the personnel security community, as there may be reason to include them as disqualifying in future versions of the adjudicative guidelines. These behaviors were then compared to the adjudicative guidelines to identify which existing guidelines could be modified to include them, or if no appropriate guideline presently exists, to suggest the creation of new guidelines to do so. A set of recommendations for improving the current guidelines was developed and included in the final chapter of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DATA FROM PUBLICLY AVAILABLE CASE STUDIES AND DOHA

A. INTRODUCTION

This chapter includes data from real-world cases of insider threat, as shown in summaries of public cases of insider threat as well as a statistical analysis of clearance denial cases from the Defense Office of Hearings and Appeals (DOHA). These two overarching sources are examined in this chapter because they are the only two ways to observe what is going on in the workforce in terms of information systems use. For the case studies section, special attention will be placed on what systems use was engaged in, such as email, file sharing, online gaming, or other activities. For the section on clearance denial cases, the emphasis will be on tallying those cases where a security clearance was denied at least initially based on misuse of information technology systems. This data will be examined from the past five years. If the general population is becoming more familiar with information technology, then over time both data sources should expect to show increases as well. Insider threat cases should have an increasing range of information systems activity, and there should be an increase in the proportion of security clearance denials based on information systems misuse.

B. CASE STUDIES

1. 2008: Gregg Bergersen

On February 11, 2008, a Chinese spy ring was broken up with arrests of Gregg William Bergersen and Tai Shen Kuo, along with another individual on espionage charges related to the passage of classified U.S. government documents and information to the government of the People's Republic of China (PRC). Bergersen lived in Alexandria, Virginia, and worked for the Defense Security Cooperation Agency (DSCA) as a weapons system policy analyst.[26] The DSCA is responsible for U.S. arms sales to foreign nations. Bergersen reportedly also held a Top Secret security clearance.

[26] Department of Justice, "Defense Department Official and Two Others Arrested on Espionage Charges Involving China," February. 11, 2008, http://www.justice.gov/opa/pr/2008/February/08_nsd_105.html.

Previously, he was the director of the Navy's command, control, communications and intelligence office.[27] In July 2008, he was sentenced to 57 months in prison.[28] According to the Federal Bureau of Prisons, he was released in November 2011.[29]

Kuo, a Taiwan-born U.S. citizen, was arrested in New Orleans along with another individual, who was passing information Kuo received from Bergersen on to a Chinese intelligence officer in Beijing. On some occasions, Bergersen received undetermined cash payments from Kuo in exchange for information and documents he provided.[30] Kuo is reported to have received $50,000 from the Chinese government for his recruitment efforts.[31] He pled guilty in May 2008 and was sentenced to 16 years in prison. Later, his sentence was reduced to five years, most likely as a result of his cooperation with the U.S. government.[32] Kuo was released from prison in June 2012.[33]

2. 2009: James Fondren

Subsequent to the arrests of Bergersen and Kuo, a retired Air Force officer and civilian pentagon employee with a Top Secret clearance, James W. Fondren, Jr., was arrested in May 2009 on espionage charges relating to his dealings with Tai Shen Kuo. He was charged with one count of conspiracy to communicate classified information to an agent of a foreign government, four counts of unlawfully communicating classified information to an agent of a foreign government, and three counts of making false

---

[27] "4 Arrests in China Spy Cases," *Washington Times*, February. 12, 2008, http://www.washingtontimes.com/news/2008/feb/12/4-arrests-in-china-spy-cases/?page=all#pagebreak.

[28] Neil A. Lewis, "Former Analyst Sentenced to Prison in Chinese Spy Case," *New York Times*, July 12, 2008, http://www.nytimes.com/2008/07/12/washington/12spy.html.

[29] Federal Bureau of Prisons, "Gregg Bergersen," *Inmate Locator*, http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=gregg&Middle=&LastName=bergersen&Race=U&Sex=U&Age=&x=0&y=0 (Accessed July 15, 2012).

[30] Department of Justice, "Defense Department Official and Two Others Arrested on Espionage Charges Involving China."

[31] Department of Energy, Counterintelligence Richland Field Office, "James W. Fondren, Jr.," http://www.hanford.gov/c.cfm/oci/ci_spy.cfm?dossier=149.

[32] "Judge Cuts Sentence of Louisiana Man who Spied for China," *Associated Press*, June 25, 2010, http://www.nola.com/crime/index.ssf/2010/06/judge_cuts_sentence_of_louisia.html.

[33] Federal Bureau of Prisons, "Tai Kuo," *Inmate Locator*, http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=tai&Middle=&LastName=kuo&Race=U&Sex=U&Age=&x=0&y=0 (Accessed July 15, 2012).

statements to the FBI.[34] Like Bergersen, Fondren had passed sensitive information to Kuo over a span of years. Fondren wrote "opinion papers" for Kuo that were often thinly veiled regurgitations of classified military reports. Fondren received $800 to $1,500 for each of these reports, which Kuo then relayed to an intelligence officer in China.[35] Fondren was convicted and sentenced on January 22, 2010 to three years in prison[36] and is currently still incarcerated.[37]

3. 2009: Stewart Nozette

Stewart David Nozette was arrested on October 19, 2009, on charges of espionage. Nozette had earned a PhD from the Massachusetts Institute of Technology in 1983, and later worked for the Department of Energy, the Department of Defense, the National Aeronautics and Space Administration and the White House's National Space Council. He had held a Top Secret clearance with access to SCI. On September 7, 2010, he pleaded guilty to attempted espionage for providing classified information to a person he believed to be an Israeli intelligence officer.[38]

Nozette had previously pleaded guilty to other charges of conspiracy to defraud the U.S. government with respect to false claims and tax evasion in January 2009, and ultimately agreed to pay restitution to the government of $265,205. During that investigation in February 2007, the FBI searched Nozette's home in Maryland and found classified documents. They later discovered that in 2002, Nozette sent an email threatening to sell classified information to Israel or another foreign government. As a result, the FBI opened an undercover operation unrelated to the original fraud case, which resulted in the subsequent espionage charges and conviction. Nozette was contacted

---

[34] Department of Energy, Counterintelligence Richland Field Office, "James W. Fondren, Jr."

[35] "Retired AF Officer on Trial in China Spy Case," *Associated Press*, September 22, 2009, http://www.airforcetimes.com/news/2009/09/airforce_spy_case_092209w.

[36] Department of Energy, Counterintelligence Richland Field Office, "James W. Fondren, Jr."

[37] Federal Bureau of Prisons, "James Fondren," *Inmate Locator*, http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=james&Middle=&LastName=fondren&Race=U&Sex=M&Age=&x=31&y=15 (Accessed July 15, 2012).

[38] Department of Justice, "Noted Scientist Pleads Guilty to Attempted Espionage," September 7, 2011, http://www.justice.gov/opa/pr/2011/September/11-nsd-1142.html.

beginning in September 2009 by undercover agents posing as Israeli intelligence officers. Through a series of meetings and dead drops, Nozette passed classified information on three occasions to what he thought was Israeli intelligence. His statements during the investigation indicated he knew the documents were classified, and that he believed his contacts to be from Israeli intelligence.[39] Nozette was sentenced to 13 years in prison[40] and is currently incarcerated in Indiana.[41]

4. 2009: Nidal Hasan

On November 5, 2009, Army Major Nidal Hasan opened fire at Fort Hood, killing 13 people and wounding 43 others.[42] A review of his personal and professional life up to that point reveals a number of activities and associations of interest. He entered the U.S. Army in the late 1980s, and after attending college, he was commissioned as a medical officer in 1997. During his medical training, his radicalization was "on full display to his superiors and colleagues."[43] In 2001, his mother died and the family held her funeral at the Dar al Hijrah mosque in Falls Church, Virginia. Anwar al-Awlaki was an imam, or religious leader, of the mosque at that time. It is unclear if Hasan personally communicated with Awlaki then,[44] though Hasan references meeting Awlaki in later email correspondence.[45] Sometime around March 2006, Hasan posted an opening online for an imam at the Walter Reed Army Medical Center, which disclosed his personal

---

[39] Department of Justice, "Noted Scientist Pleads Guilty to Attempted Espionage."

[40] Del Quentin Wilber, "Maryland Scientist Stewart Nozette Sentenced for Passing Secrets to Supposed Mossad Agent, Expresses Regret," *Washington Post*, March 31, 2012, http://www.washingtonpost.com/blogs/crime-scene/post/maryland-scientist-stewart-nozette-sentenced-for-passing-secrets-to-mossad-expresses-regret/2012/03/21/gIQAPh52RS_blog.html.

[41] Federal Bureau of Prisons, "Stewart Nozette," *Inmate Locator*, http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=stewart&Middle=&LastName=nozette&Race=U&Sex=U&Age=&x=0&y=0 (Accessed November 14, 2012).

[42] Federal Bureau of Investigation, *Final Report of the William H. Webster Commission on The Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009*, July 12, 2012, 62, http://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission.

[43] U.S. Senate, Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb*, 8.

[44] "Milestones: Nidal Malik Hasan," *New York Times*, November 7, 2009, http://www.nytimes.com/interactive/2009/11/07/us/20091107-HASAN-TIMELINE.html.

[45] Federal Bureau of Investigation, *Final Report of the William H. Webster Commission*, 50.

identity, his military affiliation, and an official military email address.[46] Starting in December 2008, however, Hasan was in regular email contact with Awlaki, which may have lasted until mid-2009 according to Awlaki himself. The first contact appears to have been through a "Contact the Sheikh" link on Awlaki's website.[47] They discussed topics such as the killing of American soldiers,[48] as well as how Hasan could safely send money to support Awlaki.[49] From publicly available reports, it is unclear if these emails were encrypted; however Awlaki is reported to have used encryption in at least some of his emails to followers.[50] Hasan joined Awlaki's website email list, and received numerous mass emails from Awlaki.[51] Post-incident searches also revealed that Hasan had multiple personal email accounts and an instant messenger account.[52] Although the FBI was aware of these emails, they did not notify the Army or Hasan's superiors, an effort which could have provided a more complete picture of the threat posed by Hasan.[53] In May 2009, a blog post attributed to Hasan supported suicide bombings and compared them with acts by soldiers who use their own bodies to shield others from exploding shrapnel. In July 2009, he purchased a gun from a local shop in Killeen, Texas, outside of Fort Hood. On November 4, the day prior to the attack, Hasan began giving away his belongings to a neighbor.[54]

As an Army officer, it was likely that he held a Secret security clearance, though no reports indicate that he accessed classified information or shared sensitive information with terrorist groups or foreign countries. While current reports do not describe the

---

46 Federal Bureau of Investigation, *Final Report of the William H. Webster Commission*, 65.

47 Ibid., 41.

48 "Al Jazeera Interview: Anwar al Awlaki Regarding Malik Nidal Hasan," *NEFA Foundation*, December 23, 2009, http://www.nefafoundation.org/miscellaneous/NEFAal-Awlaki1209.pdf (Accessed July 15, 2012).

49 Federal Bureau of Investigation, *Final Report of the William H. Webster Commission*, 54.

50 Catherine Herridge, "American Cleric Used More than 60 Email Accounts to Reach Followers, Including Hasan," *Fox News*, June 15, 2012, http://www.foxnews.com/politics/2012/06/14/al-awlaki-used-dozens-email-accounts-to-reach-followers-including-hasan/.

51 Federal Bureau of Investigation, *Final Report of the William H. Webster Commission*, 63.

52 Ibid., 66.

53 U.S. Senate. Committee on Homeland Security and Governmental Affairs. *A Ticking Time Bomb*, 8.

54 "Milestones: Nidal Malik Hasan," *New York Times*.

information that was known to Army personnel security adjudicators, it is likely that they were also not aware of the full extent of the concern that Major Hassan posed to national security.

5. 2009: Walter and Gwendolyn Myers

On June 4, 2009, the FBI arrested Walter Kendall Myers and his wife, Gwendolyn Myers, on charges of serving as illegal agents of the Cuban government for nearly 30 years and conspiring to provide classified U.S. information to the Cuban government.[55] Walter Myers earned a PhD from Johns Hopkins University,[56] and began his work at the State Department in 1977 as a contract instructor at the Department's Foreign Service Institute (FSI) in Arlington, Va. In 1978, he visited Cuba, and was later recruited by Cuban Intelligence along with his wife after his return to the United States. He was advised to seek a position within the State Department or CIA that had access to classified information. He received a Top Secret security clearance in 1985. From 1988 to 1999, in addition to his FSI duties, he performed periodic work for the State Department's Bureau of Intelligence and Research (INR). In 1999, his clearance was upgraded to include access to SCI.[57] He began working full-time at the INR and, from July 2001 until his retirement in October 2007, he was a senior European analyst, where he specialized in intelligence analysis on European matters and had daily access to classified information. The couple spent nearly 30 years providing sensitive and classified information to the Cuban government.

In April 2009, the FBI conducted an undercover operation in which Walter Myers was contacted by an undercover agent posing as a Cuban intelligence officer. Over a series of meetings, Myers described how he and his wife had passed classified information, met with Cuban agents in the U.S. and overseas and received taskings from

---

[55] Department of Justice, "Former State Department Official and Wife Arrested for Serving as Illegal Agents of Cuba for Nearly 30 Years," June 5, 2009, http://www.justice.gov/opa/pr/2009/June/09-nsd-554.html.

[56] Pete Yost, "Cuban Spies: Kendall Myers, Gwendolyn Myers Face Prison," *Huffington Post*, July 16, 2010, http://www.huffingtonpost.com/2010/07/16/cuban-spies-kendall-myers_n_648683.html.

[57] Department of Justice, "Former State Department Official and Wife Arrested."

Cuban intelligence over short-wave radio.[58] Myers is also reported to have sent encrypted emails using Internet cafes,[59] and agreed to pass information to the undercover agent using code words and encryption programs over email.[60] Walter Myers pleaded guilty in November 2009, and was sentenced to life in prison on July 16, 2010. Gwendolyn Myers received five years and nine months.[61] Both are presently incarcerated.[62]

6. 2010: Bradley Manning

In May 2010, Bradley Manning was arrested in Iraq on charges relating to the transfer of over 250,000 classified documents to Julian Assange, who then posted the documents for public view on a public website, WikiLeaks.[63] Prior to his military service, Manning displayed instances of questionable conduct. He was fired from his job at a software start-up company in late 2005 or early 2006. The company co-founder explained that it was because of odd behavior, suspected drug use, trouble focusing on work, and difficulty communicating.[64] In March 2006, the police were called when he threatened his stepmother with a knife in their home. He moved out shortly thereafter.[65]

---

58 Department of Justice, "Former State Department Official and Wife Arrested."

59 Yost, "Cuban Spies."

60 Department of Justice, "Former State Department Official and Wife Arrested."

61 Carol Cratty, "Former State Department Official Sentenced to Life for Spying for Cuba," *CNN*, July 16, 2010, http://articles.cnn.com/2010-07-16/justice/spy.couple.sentenced_1_kendall-myers-cuban-agents-gwendolyn-steingraber-myers?_s=PM:CRIME.

62 Federal Bureau of Prisons, "Walter Kendall Myers," *Inmate Locator*, http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=walter&Middle=kendall&LastName=myers&Race=U&Sex=M&Age=&x=0&y=0 (Accessed November 14, 2012).; and Federal Bureau of Prisons, "Gwendolyn Steingra Myers," *Inmate Locator*, http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=gwendolyn&Middle=&LastName=myers&Race=U&Sex=U&Age=&x=36&y=23 (Accessed November 14, 2012).

63 Kevin Poulsen and Kim Zetter, "U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe," *Wired*, June 6, 2010, http://www.wired.com/threatlevel/2010/06/leak/.

64 Ellen Nakashima, "Bradley Manning is at the Center of the WikiLeaks Controversy. But Who is He?" *Washington Post*, May 4, 2011, http://www.washingtonpost.com/lifestyle/magazine/who-is-wikileaks-suspect-bradley-manning/2011/04/16/AFMwBmrF_story_4.html.

65 Ibid.

Manning joined the Army in October 2007, graduated from intelligence analyst training, received a Top Secret clearance with SCI access, and was stationed at Fort Drum, NY. While there, his supervisor required him to seek mental health counseling due to showing signs of instability.[66] Manning was almost left behind when his unit deployed due to supervisors' perceptions that he posed a risk to himself or others. However, the unit was short on intelligence analysts and his behavior began to improve, so he accompanied his unit to Iraq in late 2009. After three months, he went home on leave, and confided in his romantic partner that he had acquired sensitive information and was considering passing it to WikiLeaks. Shortly after returning to Iraq in February 2010, WikiLeaks began posting documents that appeared to be leaked from inside the government. Not long after a classified video of a U.S. helicopter attack was posted on WikiLeaks, Manning emailed friends and was very interested in whether or not the video was getting any attention.[67] Manning is also suspected of installing unauthorized software onto a classified computer network during this time period, which enabled him to gain unauthorized access to information that was later posted on WikiLeaks.[68] Manning is suspected of sharing hundreds of thousands of classified files with WikiLeaks,[69] which exposed some of the inner workings of the U.S.-led wars in Iraq and Afghanistan as well as of international diplomacy. At the same time, however, U.S. Secretary of Defense Robert Gates downplayed the impact of the leaks, saying in a November 2010 press conference, "Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest."[70]

---

66 Ellen Nakashima, "Bradley Manning is at the Center of the WikiLeaks Controversy. But Who is He?" *Washington Post*, May 4, 2011, http://www.washingtonpost.com/lifestyle/magazine/who-is-wikileaks-suspect-bradley-manning/2011/04/16/AFMwBmrF_story_4.html.

67 Ibid.

68 Ibid.

69 "Bradley Manning Faces Court-martial in WikiLeaks Case," *CNN*, February 3, 2012, http://articles.cnn.com/2012-02-03/justice/justice_wikileaks-manning-court-martial_1_bradley-manning-david-coombs-julian-assange?_s=PM:JUSTICE.

70 Craig Whitlock, "Gates: Warnings of WikiLeaks Fallout Overblown," *Washington Post*, November 30, 2010, http://voices.washingtonpost.com/checkpoint-washington/2010/11/the_obama_administration_has_w.html.

On May 7, 2010, Manning was found laying in a fetal position in a storage closet, and later punched a female coworker in the face. He was demoted due to the assault, and was assessed by the unit psychiatrist as having an "occupational problem and adjustment disorder with mixed disturbance of emotions and conduct."[71] The psychiatrist recommended that he be discharged from the Army. His weapon was disabled, and he was transferred to work in the supply room. Manning then sought media contacts through social networking sites and made contact with a known convicted hacker, and confided in him that he had obtained State Department cables and other sensitive information. That convicted hacker notified the FBI, a tip which eventually led to Manning's arrest.

7. 2012: Jeffrey Delisle

In January 2012, a Canadian naval intelligence officer was arrested for passing classified information to Russia from July 2007 until the time of his arrest.[72] The officer, Jeffrey Delisle, most likely held a Top Secret security clearance with access to codeword program information,[73] similar to the U.S. SCI. According to one report, the volume of information disclosed by the breach was comparable to the volume of U.S. data loss to WikiLeaks.[74] Delisle was charged with communicating information to a foreign entity that could harm national interests, a charge under a section of the Security of Information Act. This is the first time anyone has been charged under that section of the act.[75] On October 10, 2012, he pleaded guilty to this charge as well as to criminal breach of trust.[76]

---

71 Nakashima, "Bradley Manning is at the Center of the WikiLeaks Controversy."

72 Kathryn Blaze Carlson, "Decoding the Case of Alleged Canadian Spy Jeffrey Paul Delisle," *National Post*, January 18, 2012, http://news.nationalpost.com/2012/01/18/decoding-the-case-of-alleged-canadian-spy-jeffrey-paul-delisle/.

73 Ibid.

74 Alistair Macdonald and Siobhan Gorman, "Canadian Military Leak to Russia Riles Allies," *Wall Street Journal*, March 28, 2012, http://online.wsj.com/article/SB10001424052702304177104577307991514394210.html.

75 Murray Brewster, "Harper Government had to Resist Urge to Blame Russia in Spy Case," *Toronto Star*, May 21, 2012, http://www.thestar.com/news/canada/politics/article/1181820--harper-government-had-to-resist-urge-to-blame-russia-in-spy-case.

76 Richard J. Brennan, "Canadian Spy Jeffrey Paul Delisle Pleads Guilty to Espionage Charges," *Toronto Star*, October 10, 2012, http://www.thestar.com/news/canada/article/1268849--canadian-spy-jeffrey-paul-delisle-pleads-guilty-to-espionage-charges.

He is pending sentencing and could face life in prison.[77] Sources in the case initially said that Delisle was motivated by money,[78] but later reports showed that he had marital issues and wrestled with thoughts of suicide. Once he began working for the Russians, he received $3,000 monthly and also became fearful for his children's safety if he did not cooperate.[79]

Additionally, Delisle is reported by his ex-wife to be an excessive computer user, Internet gamer, and collector of medieval fantasy gear. He is said to have admitted to having a computer addiction. A Canadian newspaper quotes her as saying, ""He played a lot of games like Ultimate Online, World of Warcraft, and Star Wars, and he actually let our kids play a lot of video games like that too."[80] She also said that Delisle would spend large amounts of money in the games, such as purchasing a virtual sword for hundreds of dollars. He made online posts indicating that he was interested in making friends in the virtual gaming communities. He also is reported to have made purchases on eBay for real-life medieval clothing such as chain mail, as well as intelligence-themed memorabilia associated with the CIA and DIA.[81] Delisle used email to communicate with his Russian handlers,[82] and appears to have used at least one social networking platform.[83] A published analysis of his computer showed that he used removable media including floppy drives and USB drives, and also employed special software[84] designed

---

[77] Richard J. Brennan, "Canadian Spy Jeffrey Paul Delisle Pleads Guilty to Espionage Charges," *Toronto Star*, October 10, 2012, http://www.thestar.com/news/canada/article/1268849--canadian-spy-jeffrey-paul-delisle-pleads-guilty-to-espionage-charges.

[78] Brewster, "Harper Government had to Resist Urge to Blame Russia in Spy Case."

[79] Terry Milewski, "5 Plot Lines in the Jeffery Delisle Navy Spy Case," *CBC News*, October 27, 2012, http://www.cbc.ca/news/politics/story/2012/10/26/jeffrey-deslisle-spy-plotlines.html.

[80] Steven Chase, Tamara Baluja, and Jane Taber, "Accused Spy Jeffrey Delisle Led Second Life Online," *Globe and Mail*, March 30, 2012, http://www.theglobeandmail.com/news/national/accused-spy-jeffrey-delisle-led-second-life-online/article4097146/.

[81] Ibid.

[82] Milewski, "5 Plot Lines in the Jeffery Delisle Navy Spy Case."

[83] "Jeff Delisle," In *MySpace*, http://www.myspace.com/493089927 (Accessed November 6, 2012).

[84] "Forensic Analysis of Delisle's Computer," *Chronicle Herald*, October 22, 2012, http://www.scribd.com/doc/110813170/Forensic-analysis-of-Delisle-s-computer (Accessed November 14, 2012).

to fully erase disk contents by overwriting them.[85] The full extent of his online and virtual activities, including whether or not he made contacts or passed information to foreign agents using such avenues, is not yet known. It is possible that as the case continues, more information will be publicly disclosed.

C. DATA FROM CASE STUDIES

As shown in Appendix B, this study examined case studies and identified forms of online behavior each individual engaged in using a list of online behaviors or activities. For each activity as identified in news articles on Internet searches, a tally was placed in the matrix. The total tally for each case is shown at the bottom of the matrix in Appendix B. The tallies for each case are shown in Figure 1, Online Activities by Case over Time. As the trend line shows, the number has increased over time, with Bradley Manning displaying an unusually high engagement in online activities. Jeffrey Delisle is reported to have engaged in an elevated number of online activities, and as the case develops there may be additional activities uncovered. It appears tentatively that in publicized cases of insider threat, the individuals are increasingly engaged in online activity.

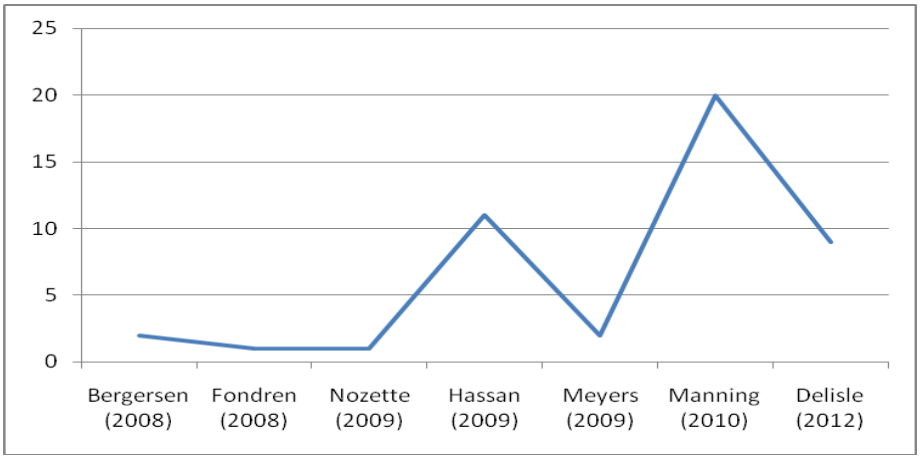

Figure 1. Number of Internet Activities in Case Studies Over Time

[85] Communications Security Establishment Canada, "Entrust TrueDelete Version 4.0 for Win95/NT," September 13, 2012, http://www.cse-cst.gc.ca/its-sti/services/cc/truedelete-v40-eng.html.

D. DATA FROM THE DEFENSE OFFICE OF HEARINGS AND APPEALS

As previously discussed, the office responsible all for security clearance appeals for contractors in the Department of Defense, as well as for 20 other federal departments and agencies, is the Defense Office of Hearings and Appeals (DOHA). This section includes a numerical tally of all DOHA cases that were denied under the personnel security adjudicative guideline, Misuse of Information Technology Systems, also known as Guideline M. The tally was then calculated as a percentage of the total cases, so that a proportion could be identified. The same five year period was selected as for the insider threat case studies. Over time, this proportion should increase as more and more applicants for security clearances would be more familiar with information systems.

In contrast to the previously-identified trend of increasing online activity, the tally of DOHA cases that used the Use of Information Technology Systems guideline actually stayed the same or decreased over the same time period. The number of cases in which the guideline for Use of Information Technology Systems was applied was 21 in 2008, 25 in 2009, 22 in 2010, 21 in 2011, and is projected to be 17 in 2012 (see Figure 2). Even when compared to the overall number of cases adjudicated by DOHA under all guidelines, the trend remains essentially flat. Given annual totals for the same years of 1647, 1540, 1514, 1516, and 1208 (projected), the respective percentages of cases which DOHA applies the Use of Information Technology Systems guideline is 1.28%, 1.62%, 1.45%, 1.39%, and 1.41% (see Figure 3).

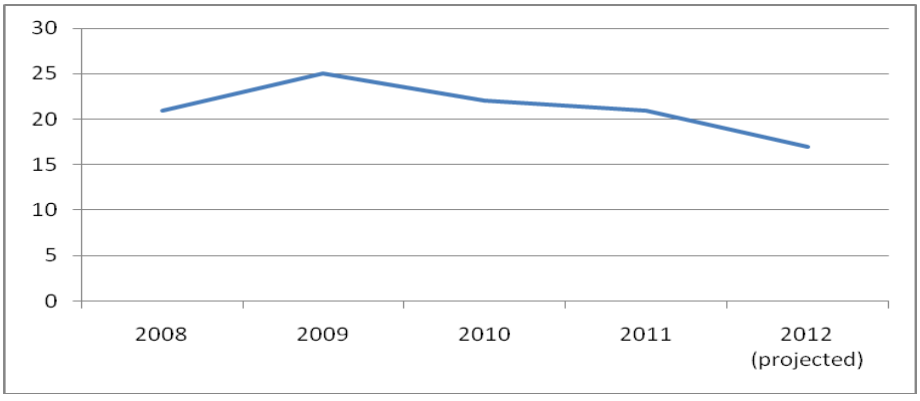

Figure 2. Number of DOHA Clearance Denial Cases for Use of IT Systems over Time

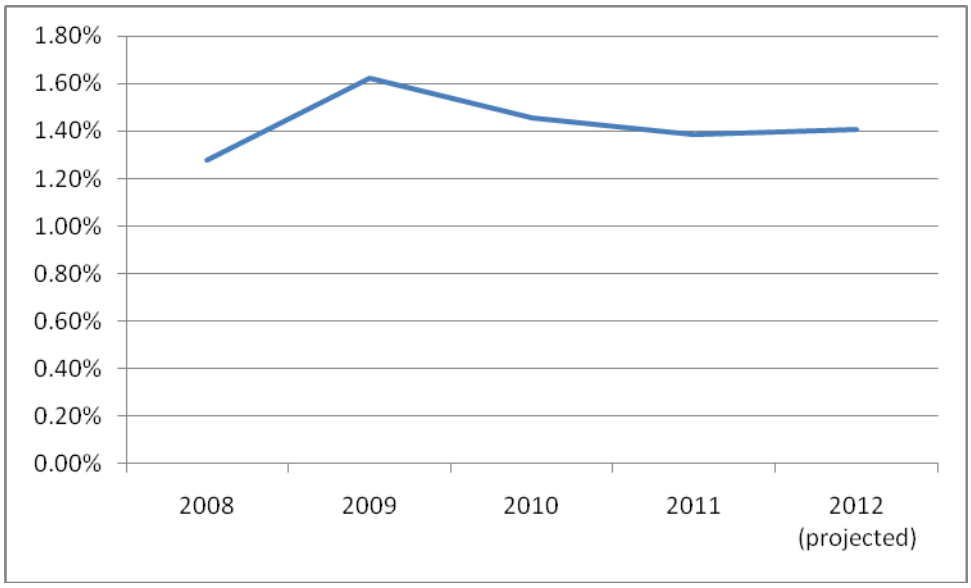

Figure 3. DOHA Clearance Denial Cases for Use of IT Systems as a Percentage of Total Cases over Time

It is unclear why there are diverging trends in these two measures of online activity. If individuals are generally becoming more connected to the Internet and have an increasing virtual presence, then it could be expected that the number of DOHA cases where individuals misused IT systems would also increase proportionally. The cleared and applicant populations may simply be engaging in fewer disqualifying behaviors over time, or more aware of what behaviors could disqualify them from obtaining a security clearance. If this is not the case, however, the difference in trends may have implications for the effectiveness of the present personnel security background investigation process which largely does not account for online searches of applicants, also known as cybervetting. Presently the standard OPM background investigations that are conducted in support of security clearance adjudications do not include even a cursory name search on a public search engine. One hypothesis for this difference could be that without an effective means to check online activity, the investigation process is catching less and less of the derogatory information available on a given applicant. So as our insider threat cases show increased online activity, the ability of those agencies and departments served by DOHA to identify related cases is proportionately decreasing. This hypothesis suggests an avenue for future research that will be discussed later in this study. A

corollary to this hypothesis is that if the government can begin to incorporate cybervetting into its background investigations, it will result in an increase in security clearance denial cases based on the Use of Information Technology guideline.

E. SUMMARY

The above two sections, Case Studies and Data from DOHA both show trends that may be significant for the personnel security community. The trend among case studies is that the variety of use of information systems by insider threats has increased over the past five years. The other trend is that security clearance denial cases brought to DOHA have generally been steady, showing no corresponding increase in the number of cases over the past five years. After an increase in 2009, the proportion of denials based on IT systems misuse has actually decreased over time. A lack of effective cybervetting was proposed as one potential explanation for this divergence, but there could be other reasons as well and future research is needed. This divergence could mean that the government is increasingly vulnerable to IT systems misuse, although it should be noted that the impact of such misuse can be difficult or impossible to measure, especially in the public domain. For example, even in the cases of Manning and Delisle, where hundreds of thousands of classified documents were exfiltrated from classified systems, there has been no public evidence of deaths, injuries, or failed military missions that resulted. Even the degree of diplomatic difficulties that the foreign policy community has encountered has been hard to measure, and the evidence has been anecdotal at best.

V. CYBER BEHAVIORS IN CASE STUDIES AND THE ADJUDICATIVE GUIDELINES

This chapter focuses on the third research goal, which examines the impacts emerging technologies have on the ability of the adjudicative guidelines to mitigate insider threat. The list of online activities in Appendix B was compared with the disqualifying conditions of the adjudicative guidelines as identified in Appendix A. For each online or information systems behavior, the guidelines were reviewed to identify what guideline and disqualifying paragraph could apply. The guideline paragraph number was recorded for any behaviors that could be addressed by an adjudicative guideline. If more than one guideline could apply, multiple paragraph numbers were recorded. This exercise was completed for all behaviors on the list, identifying those online behaviors that were covered by the adjudicative guidelines and those that were not. Appendix B also includes which of the insider threat cases are publicly reported to have engaged in each behavior.

A. ROUTINE AND SITUATIONAL USES

This section is devoted to activities that by themselves may not represent a concern, but given other factors or contexts become problematic. Social uses of information technology such as email, text messages, or social networking are generally routine and benign, but become problematic when they enable a person to connect with foreign governments or terrorists, pass sensitive information, or have other negative consequences. Personal computer uses that are routine or social when done in private may not be appropriate or acceptable in the workplace. Additionally, lax information systems security habits such as not updating virus software or writing down passwords by themselves may be harmless without external threats that exploit them, such as malicious code or a foreign intelligence service. Beyond lax habits, there are activities proactively taken to circumvent security policies and measures, which could be problematic when done for malicious purposes.

1. Social and Routine Uses of the Internet

This category includes behaviors that are widely engaged in by the public, as individuals use the Internet to connect with family and friends, and to meet new people. Examples of such routine or social uses include using email; posting to bulletin boards, web logs, or chat rooms; online gaming; online dating; using Voice over Internet Protocol (VoIP); using social media platforms; online shopping for real or virtual goods; or sending text messages. Other more sophisticated practices may also fall into this category, including using encryption on emails, advanced file overwrite software, or using IP proxies or routers without the user allowing their own computer to be used by others as a proxy or router. By themselves, these behaviors are routine and would not present an increased risk for adjudication of security clearance according to the Adjudicative Guidelines. However, they could facilitate or help to hide other disqualifying behavior. This could include making foreign contacts on a social networking site, communicating with terrorist groups using encrypted communications, or targeting a malware attack via a proxy server to mask an individual's identity.

Since 2008, social and routine use by the individuals in the examined case studies has increased. Bergersen, for example, is known publicly to have used email and encrypted communications prior to his arrest in 2008, while more recent cases have shown a wider array of social or routine use. Bradley Manning is reported to have used email, instant messaging, social network platforms, encrypted communications, and removable media devices, while Delisle is reported to have been part of virtual communities and made online purchases of real and virtual goods. It is also likely that someone with Delisle's familiarity with the Internet and virtual worlds would have also been a regular user of email, instant messaging, and social networking platforms, and possibly familiar with the use of encrypted communications and proxy servers or routers. As the details of the case become clearer, more information on Delisle's routine and social Internet use may become public.

2. Unauthorized Activities in the Workplace

Employees in today's workplaces are often given computers and access to the Internet to perform their duties. However, this can present opportunities for individuals to misuse these resources. This category of online behavior can include viewing inappropriate or unauthorized websites while at work, downloading large files on employer bandwidth, hosting or playing online games, misusing employer email accounts, using employer computers for personal business, or other computer-related misuse of employer time or resources. It should be noted that the intentional disclosure of classified information, while usually work-related in some way, will be discussed separately in a later section. Without knowing more about the specific rules of behavior in place for each of the case studies examined, it is difficult to identify the extent to which those individuals engaged in this category of activity. For example, unless the blogs and social networking sites that Bradley Manning used were specifically identified and banned by the Army, and unless he used a duty-only computer (as opposed to computers made available to soldiers for personal uses such as writing home or checking finances), he may not have engaged in activities covered in this section.

While there is no specific guideline for employee misconduct (such as in the employment suitability regulation, 5 CFR 731, which include a disqualifying factor for "misconduct or negligence in employment"[86]), many of these examples could fall within the Personal Conduct adjudicative guideline. Specifically, online activities in the workplace, when in violation of written rules of behavior, could be disqualifying under section 16(e), if it constitutes "a pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency." This language implies that more than one instance of a violation is needed in order to constitute a pattern, and that this only applies to employment with a federal agency and not in cases of rule violations while employed at a private company.

86 "Criteria for Making Suitability Determinations," Code of Federal Regulations, Title 5, Pt. 731.202, Electronic Edition, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=5:2.0.1.1.7&idno=5#5:2.0.1.1.7.2.1.2 (Accessed November 14, 2012).

3. Improper or Poor Information Systems Security Habits

This category includes those behaviors that show a lack of adherence to widely-accepted security practices, which could create vulnerabilities for an individual or those people, companies, or organizations the individual is associated with. This thesis organizes such habits into five categories: online browsing habits, email and messaging habits, password management, network connections, and system security. Each category has its own implications for personnel security and the adjudicative guidelines. None of the case studies that were examined show any specific indicators of lax security habits of individuals leading to damage to the national security, though it is possible in the Manning and Delisle cases that coworkers, supervisors, or network administrators failed to take steps that would have mitigated some of the vulnerabilities that were later exploited.

Online browsing habits can include behaviors such as accepting invalid secure socket layer (SSL) certificates, clicking on unknown web links, downloading files or software from unknown or untrusted sources, purchasing goods from unknown sources, sharing personal or financial information with untrusted sources, or using unsecure connections. This kind of activity could leave a user unprotected or create vulnerabilities, but a review of the Adjudicative Guidelines shows no clearly applicable disqualifying factor. Email and messaging habits can include opening an email or attachment from an unknown sender, opening or responding to spam emails, sending personal or financial information to an unknown recipient. The Adjudicative Guidelines do not appear to cover this category, either. Lax password management can include using weak passwords for personal accounts, using the same password across multiple accounts, never changing a password, sharing passwords with others, not protecting passwords, or using simple or easily-guessed password recovery questions. Again, there are no clearly applicable adjudicative guidelines for this kind of behavior.

Keeping network connections secure and using them properly protects individuals and information. Lax habits in this area could include connecting to unsecure wireless access points such as those found in airports or hotels, maintaining an open wireless router for personal use, or allowing a personal computer to serve as a proxy or exit point

for other unidentified users. In the Tor router network, for example, computers are voluntarily used in a series of IP address relays, with some computers voluntarily serving as exit points for Internet traffic. Thus the true identity of the user is concealed behind layers and layers of intermediary IP addresses with only the last address being visible to the target website. Such a network facilitates individuals in repressive countries to speak freely without facing political arrest, but can also facilitate criminal activity and hinder legitimate law enforcement investigation. This would be akin to an individual lending their vehicle to anyone else without question; doing this might help someone in need, but it also creates an obvious vulnerability that the vehicle could just as easily be used to facilitate an armed robbery or terrorist attack. Allowing a computer IP address to be used as such a relay exit point or proxy for other users not only makes the individual vulnerable to malicious actors, but could also facilitate criminal activity if their IP address is used by criminals to access illegal content or facilitate clandestine communications. In that case, Personal Conduct paragraph 16(g), "association with persons involved in criminal activity," could apply.

Lax system security behaviors include failing to install or update anti-virus or other security software, failing to update software with newer versions or patches, reducing browser security settings, synchronizing with unsecured mobile devices, using programs that allow remote or mobile access to a personal computer, or unintentionally installing unauthorized software onto an official or classified computer system. The last item may call for workplace counseling, and could become disqualifying under the Adjudicative Guidelines if the behavior continued despite that counseling. Specifically, paragraph 34(h) includes "negligence or lax security habits that persist despite counseling by management." Otherwise, these activities do not appear to be presently covered. The wording from paragraph 34(h) implies that the lax habits are only applicable to the workplace, or else management would not be in a position to provide counseling. It also implies that the behavior by itself is not disqualifying unless the individual is counseled; absent formal counseling, the individual can continue the behavior without consequence for their security clearance. Therefore, this discussion of lax security habits in an

individual's nonprofessional life, and without training or counseling, does not have an impact on his or her security clearance under the present Adjudicative Guidelines.

The examination of lax security habits raises a number of challenges for personnel security. It may be difficult to argue that an applicant should potentially be denied a security clearance because they don't use a strong password on their home wireless router, or because they use the same password in multiple personal accounts. Furthermore, the ability to question or investigate these areas may be limited without requiring disclosure of personal account password information to security officials, a practice which may be inadvisable or even illegal. Such security habits may also be common enough to preclude taking unfavorable actions regarding a security clearance. As individuals are free to leave the doors to their homes unlocked, or walk alone at night, so too can individuals make choices with their personal online behavior that increase their vulnerability.

On the other hand, this activity may be disqualifying under Personal Conduct paragraph 16(d), if it becomes "credible adverse information that is not explicitly covered under any other guideline… which… supports a whole-person assessment of questionable judgment… or other characteristics indicating that the person may not properly safeguard protected information." The key challenge for security clearances is to determine the line at which a lax security habit crosses from forgivable naiveté to unforgivable negligence that is significant and obvious to a reasonable person, as well as whether or not personnel security specialists need more specific guidance when deciding where to apply this line in case adjudications.

4. Improper or Poor Operations Security (OPSEC) Habits

This category includes behaviors and practices that could jeopardize the operational security of the user of the agency or company they work for. This could include giving too much personal detail such as social security numbers or full dates of birth on social networking sites, posting information that links the user to their employer, exposes the physical locations of company or agency worksites, discusses physical security posture or procedures, posting geographically tagged pictures with embedded

location coordinates, or posting operational information on resumes or job applications. Bradley Manning engaged in this type of activity when he discussed with an online associate who he had never met his work as an intelligence analyst, his access to classified information, and how his office had "weak servers, weak logging, weak physical security, weak counterintelligence, and inattentive signal analysis ... a perfect storm."[87]

Poor use of operational security could be considered under the Handling Protected Information paragraphs 34(a), (b), (c), and (h), but only if the operational data is considered "protected information." This is unclear, as the fact that an employee works for a certain agency, the grid coordinates or floor plan of an office, or the duty hours of the gate guards are likely not considered classified or official use only. Unless the information is considered as protected, this activity is not disqualifying under this guideline. The only other guideline that could be applied is the Personal Conduct paragraph 16(d) as it could constitute questionable judgment or an unwillingness to comply with rules and regulates, but only if the individual's company or agency specifically outlines what information is allowed to be posted online or in social networking sites.

B. FURTHERING ILLICIT ACTIVITIES

As previously established, this paper has identified three main categories within which the list of cyber activities may fall. The first category contains uses of Internet technology to further other illicit activities. Specifically, this includes explicit or offensive activities, intentional disclosure of classified or sensitive information, the use of the Internet to commit crimes, employment of false identities, and engagement in bullying online behavior. Each of these areas will be briefly examined for its significance to the personnel security discipline as well as through an examination of case studies.

87 Ellen Nakashima, "Bradley Manning is at the Center of the WikiLeaks Controversy."

1. Explicit, Obscene, or Offensive Activities

This category includes activities that a third party might deem inappropriate, obscene, or offensive. Examples include accessing extremist websites or online pornography, sending spam messages with offensive text or pictures, or sharing images of sexual activity or violence. Excluded from this category are activities engaged in at the workplace, which would be covered under the Unauthorized Activities in the Workplace category. A review of the publicly available information pertaining to the identified case studies shows no known engagement in such activity. While it may be highly likely the Nidal Hasan viewed Jihadist or other extremist websites or viewed or shared images of violent activity, this was not affirmatively supported in the case study research.

Such obscene activities, when done on a personal computer away from the workplace, may not constitute illegal behavior and may be protected free speech. The present adjudicative guidelines do not address this kind of behavior unless it is conducted at the workplace or violates a law. In those cases, Personal Conduct paragraph 16(d)(2) and (4), or Criminal Conduct paragraph 31(a) and (c) could apply.

2. Intentional Disclosure of Classified or Sensitive Information

When classified or official use only information is knowingly shared with individuals without proper clearance and need to know, damage to national security can occur. Activity that involves such intentional disclosure can include emailing or instant messaging classified information with foreign nationals, downloading classified information to an unclassified system or network, sending classified or sensitive information to a website or blog, or posting classified information on an unclassified resume. Bradley Manning is the only case example that has engaged in such behavior. He is reported to have engaged in sending classified emails and instant messages to uncleared individuals and foreign nationals, downloading classified information to an unclassified system, and sending classified information to a website.

The adjudicative guidelines appear to address this behavior very well. Handling Protected Information paragraphs 34(a), (b), (c), and (g) applied to almost all activities under this section, and paragraph 34(f) applied to some in addition. When classified or

sensitive information is disclosed to foreign nationals, Foreign Influence paragraph 7(a) and (b) also apply. Depending on the allegiances or intentions of the recipient, Allegiance to the United States paragraphs 4(b) and (c) could also apply. There were no example behaviors considered in this section that were not readily addressed in the adjudicative guidelines.

3. Criminal Activity

The Internet's ability to connect individuals and networks makes it a key medium for both legal and illegal activity. Crimes can be more easily committed using the Internet, including the acquisition and sharing of illegal pornography, intellectual property, proprietary information, software licenses, stolen items, stolen identities, laundered money, or financial support to terrorism. The Internet can also facilitate crimes such as fraud, including toll fraud committed through phone "phreaking" tactics such as switch-hooking.[88] The cases examined showed no known engagement in this kind of activity. By the nature of the activities included in this section, Criminal Conduct paragraphs 16(a) and (c) could apply to all activities. In cases where child pornography, encounters with minors, or prostitution are involved through online downloading or solicitation, Sexual Behavior paragraphs 13(a) and (c) could apply. Money laundering and financial support to terrorism (also known as reverse money laundering) could be addressed in Allegiance to the United States paragraph 4(a), (b), and (c). If there is a foreign nexus to any of the activity, Foreign Influence paragraphs 7(a), (b), and (g) could also apply.

4. Use of False or Misleading Identities

This category can include the use of misleading or false identities online, such as participating in a chat room or group with a fake identity, creating misleading email accounts, using another person's accounts or passwords, falsifying online resumes, or associating oneself with a company or organization that he or she is not a part of.

88 "Chapter Nine: Phone Phreaking in the U.S. & UK," In *A Complete Hacker's Handbook: Everything You Need to Know about Hacking in the Age of the Web*, 1st Edition, http://www.telefonica.net/web2/vailankanni/HHB/HHB_CH09.htm.

Additionally, this category could include more technical misrepresentation such as spoofing email addresses or altering email headers to appear to come from another person or IP address. For the purposes of this research, case studies were reviewed for examples of deliberate falsification rather than simply anonymizing one's identity instead of using the user's real name, which could be interpreted as a best practice for personal safety on the Internet. None of the cases examined showed deliberate falsification or use of another person's identity, though Manning and Delisle used anonymous screen names to communicate, and it is likely that Nidal Hasan did so as well.

The adjudicative guidelines do not explicitly address the use of false identities, other than when engaged in during a background investigation, hiring process, or other official personnel or security process. A pattern of dishonesty or rule violations in the workplace could be disqualifying, but this appears to be limited to the workplace. It is possible to interpret Personal Conduct paragraph 16(d) to include "untrustworthiness" as part of a whole-person assessment that disqualifies the applicant, but this may not be clear. The example of falsifying a resume would likely be included in this paragraph, but other uses of false identities online are not clearly disqualifying. The only other applicable guideline is Criminal Conduct paragraphs 31(a) and (c) if the false identity violated the law, such as in the case of fraud. However, it may not always be readily apparent when a given behavior crosses this line.

5. Bullying, Intimidating, or Threatening Behavior

Online activity that is hurtful or threatening to a person or group of persons can include hosting a website or making online comments to damage an employer or its employees, posting hurtful information or pictures of someone without their permission, or harassing or bullying someone online. Nidal Hasan is reported to have communicated with Anwar al Awlaki to discuss killing American soldiers, and is also reported to have made a blog posting about suicide bombers. Bradley Manning facilitated the posting of information that was damaging not only to the United States government, but to foreign diplomats and other leaders whose private deliberations were made public. In the wake of the WikiLeaks disclosure and during the Occupy Wall Street protests in Fall 2011, some

hacker groups such as Anonymous engaged in menacing behavior by posting personal information of targeted individuals and their family members online, a practice referred to as "doxing."[89] While this personal information was publicly available in various places on the Internet such as white pages or social networking profiles, it was collected and posted in a "dox," such a way that suggested the targeted individual could be harassed or bullied by anyone wishing to do so.

Unless the menacing behavior violates the law, the adjudicative guidelines do not address it. When criminal, Criminal Conduct paragraphs 16(a) and (c) could apply. One example of such behavior could be "swatting," a term used to describe when a person calls for emergency services to false emergencies in order to disrupt legitimate services, waste government resources, and put innocent victims and responders at risk, often by using software programs that hide the caller's true identity and location. This kind of menacing activity is widely illegal, and a number of violators have been convicted and received jail sentences.[90] If a person's sensitive information such as social security number are revealed in the course of the behavior, it could be included under Handling Protected Information paragraph 34(a) and (b); it is not readily clear, however, if this kind of information is included as "protected" as it is not considered classified or for official use only, or other category of government protection. It is likely, however, the individual whose social security number is exposed, would consider it protected and not authorized for public disclosure.

C. USES OF TECHNOLOGY SPECIFIC TO THE INTERNET

The third section of this thesis includes the malicious uses of technology that are specific to the Internet. These are activities that involve, take place within, and directly impact the information technology environment. These activities are not routine or social uses, and are not in furtherance of traditional activities, but are themselves dependent on the technology itself. That is, there could be no unauthorized access to information

89 Steve Ragan, "The FBI's Warning about Doxing was Too Little Too Late," *Tech Herald*, December 19, 2011, http://www.thetechherald.com/articles/The-FBIs-warning-about-doxing-was-too-little-too-late.

90 Michael Cooney, "FBI Warns Emergency 911 Swatters are a Growing Menace," *Network World*, February 5, 2008, http://www.networkworld.com/community/node/24714.

systems or network sabotage without the existence of the information systems and networks in the first place. What follows is a discussion of each of those categories.

1. Gaining Unauthorized Access and Bypassing Security

Activities in this category include hacking or other means to gain unauthorized access to information systems or networks. Some examples include hacking into another person's email account, obtaining account passwords using social engineering, spyware, or keylogger software, installing software that facilitates unauthorized access, using administrator or other "back door" entry points without permission, or using one system to help gain access to another system in an unauthorized manner. Bradley Manning is accused of hacking into government computer systems by using unauthorized software to gain access to classified information that he otherwise was not authorized to access. No other case studies showed that the individuals in question had obtained unauthorized access.

The adjudicative guidelines are generally very thorough in their coverage of this category of activity. Use of Information Technology Systems paragraphs 40(a), (c), (e), and (f) are commonly applicable, and paragraph 40(b) and (d) were also applicable to some activities. Manning's activity is specifically disqualifying under 40(c) and (f) as the use of an information technology system to gain unauthorized access to another system, and the introduction of software onto a system without authorization. Activities in this category that had no applicable adjudicative guideline included port scanning and network reconnaissance, visiting hacker websites to learn techniques, and researching system or network vulnerabilities. These activities, while concerning, are not disqualifying under any guidelines unless an individual takes further malicious actions as a result of this research, or there are explicit workplace rules that prohibit the activity.

This category also includes the intentional bypassing of security measures, such as using unauthorized proxy servers; lowering security settings on an Internet browser; and disabling firewalls, anti-virus software, event logging, or other security safeguards. Public information on the examined case studies showed no confirmed engagement in this type of conduct. The adjudicative guidelines do address this under Use of

Information Technology Systems paragraphs 40(b) and (g), which include unauthorized modification of system software, and negligence or lax security habits.

2. Computer Network Sabotage

Activities included in this category have the intent of injuring or attacking websites, software, hardware, or the smooth operation of the Internet or local networks. Examples include making changes to a website, conducting denial of service attacks on websites, using botnets, releasing malicious code such as worms, viruses, or Trojans, using malware to damage or destroy a system, or otherwise sabotaging a computer or network. Related to these activities is the sharing of network security information with a hacker group or other individuals with the explicit or implicit understanding that it could result in similar damage. None of the case studies showed this form of behavior; the individuals may have been more interested in exploiting their networks than simply bringing them down.

The Use of Information Technology Systems guideline, especially paragraphs 40(a) and (b) are applicable to most of this activity. In the cases of introduction of hardware or software onto a system, 40(f) also applies. The transmission of network information to a hacker group is not included in the Use of Information Technology Systems guideline, but could be applicable under Handling Protected Information, paragraph 34(a). The only activity without an applicable guideline is the setting up of fake accounts on a website in order to clog its customer list. This may not be illegal, and does not require unauthorized access to any system. However, it would arguably take more effort to set up such accounts than it would be to identify and delete them, leading to a potential net loss of return on investment for engaging in the activity.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. DISCUSSION AND RECOMMENDATIONS

This chapter will discuss the previous information and its implications for the personnel security adjudicative guidelines, and provide specific recommendations for enhancement. It reviews the current state of personnel security by assessing how the online behaviors compared to the adjudicative guidelines. This includes which guidelines were generally well covered, partially covered, or not covered. Given that assessment, the section proceeds to describe recommended changes to the adjudicative guidelines in order to address those areas assessed as partially covered or not covered. By making these changes, the personnel security community may be better able to mitigate insider risks such as espionage or terrorism involving cleared personnel. This chapter also includes a discussion of the limitations of this research, followed by this thesis' concluding comments.

A. THE CURRENT STATE OF SECURITY

Of the eleven categories of online behavior contained in the list developed by this study, the present adjudicative guidelines effectively address four, and mostly address one, but do not address the remaining six. As shown in Appendix B, there is widespread coverage of at least one adjudicative guideline paragraph in the categories of unauthorized workplace use, intentional disclosure of sensitive information, use of the Internet to commit other crimes, and use of the Internet to commit network sabotage. The present personnel security adjudicative guidelines appear to provide sufficient and clear tools for agencies to disqualify individuals engaged in these forms of online activity.

One category has significant coverage but with three specific activities that are not addressed. In the unauthorized access and bypassing security category, conducting vulnerability research on networks, port scanning and network reconnaissance, and visiting hacker websites in preparation of hacking were not addressed by the guidelines, as they were not illegal or actively destructive in nature. This activity may be concerning, however, as it may show a malicious intent to damage network systems. It may be possible that an individual engaged in this activity may be at a heightened risk of

engaging in more serious, damaging, or criminal activity in the future and may be less inclined to protect classified or sensitive information in the workplace.

The guidelines do not address six of the categories of online use, including social use, lax security habits, operations security, obscene activity, false identities, and menacing behavior. In reviewing the categories that are contained in the social or routine use section, it is likely that most if not all of the activity in the social use and obscene activity categories could be considered free speech and is engaged in by significant portions of the population. It is unclear what, if any, effort could be undertaken in the adjudicative guidelines to address this activity. The remaining categories may suggest additional discussion.

Lax security habits include activity such as following unknown links in emails, downloading files from untrusted sources, and other legal but unsafe personal computing habits. The present adjudicative guidelines do not address these behaviors, but they could be harmful to employees' personal computers or information. They could potentially put an individual at risk for blackmail or coercion as malicious actors could obtain their personal information more easily from such vulnerabilities. It also may show poor judgment or lack of familiarity with the Internet or online communications, which in today's world could be a concern relating to a person's ability to safeguard classified or sensitive information. A similar concern is present in the operations security category, as individuals who are posting locations, building layouts, or pictures that contain grid coordinates may be inadvertently helping a malicious actor to damage the government's assets or operations, and may show poor judgment in protecting sensitive information.

The guidelines also do not account for the use of false identities unless they are used for fraud or other crime, or are related to employment or background investigations. The use of the Internet provides increasing opportunities for people to misrepresent themselves, so this could be more of an issue as technology develops. Lastly, the guidelines do not address menacing online behavior unless it becomes criminal or involves the publishing of sensitive information. This means that malicious doxing, cyberbullying or other harassment, or spreading false rumors about a person is not readily addressed. These behaviors may be concerning in light of the responsibility, public

exposure, and trust placed in applicants for security clearances. Individuals engaging in this type of behavior may use their increased access to expose even more personal information about others or increase the effectiveness and reach of their intimidation or harassment efforts. Public knowledge that an individual with a history of such behavior was hired and granted a security clearance may also be embarrassing for the agency or company. Presently the adjudicative guidelines only address false information if it relates to the background investigation or hiring process, and not in other areas of a person's life. The guidelines also do not address non-criminal activity, and in the world of online bullying the line between pointing out a person's physical flaws or fabricating a sexual encounter and criminal harassment may be a grey area not explicitly addressed.

B. RECOMMENDED UPDATES TO ADJUDICATIVE GUIDELINES

Given the above discussion of the categories of online activity and the adequacy of the personnel security adjudicative guidelines, there are implications for several existing guidelines as well as one potential new guideline. This section will discuss the implications for each guideline.

1. Foreign Influence

Foreign influence was identified as a guideline that could apply to the intentional disclosure of sensitive information to foreign nationals as this could be a contact that creates a heightened risk for foreign exploitation or be a connection that creates a conflict of interest between the individual's obligation to protect sensitive information and their desire to help their foreign associate. The definition of "contact" or "connection" may be evolving with the expanding numbers of relationships individuals can form on the Internet, as may be the word "association," which is also used in paragraphs 7(f) and (g). Inclusion of more specific language may help clarify this guideline. This guideline may benefit from more specific guidance regarding which associations are disqualifying in the online world, such as being friends with a foreign national on a social networking site.

2. Financial Considerations

While no online activity examined was addressed using the Financial Considerations guideline, the case studies reiterated the importance of this guideline in addressing insider threat cases. Derogatory information under the Financial Considerations guideline was found in the case study reviews of Jeffrey Delisle, who may have needed money to fund his online gaming and other purchases by selling information to the Russian government; Gregg Bergersen and James Fondren received money from the Chinese government for their sensitive information, though it is unclear if they were experiencing financial difficulties; and Stuart Nozette had previously been convicted of tax evasion charges and owed the government more than $260,000 dollars. This guideline continues to be important in identifying and mitigating insider threat. However, the Delisle case information may suggest an area for strengthening the Financial Considerations guideline by adding language that includes debts due to excessive online gaming excessive participation in virtual worlds, or excessive use of virtual currency.

3. Personal Conduct

The Personal Conduct guideline had frequent application in the unauthorized workplace use and furtherance of criminal activity categories. There were other areas in which it may have been applicable if those areas included activity at the workplace or the conduct of a background investigation. The guideline covers behavior that could raise questions about an individual's judgment, trustworthiness, or reliability, as well as behavior that could be disruptive, violent, or otherwise inappropriate in the workplace. By expanding the language in this guideline to explicitly include all false or purposely misleading information, as well as disruptive, violent or other inappropriate behavior, the guideline could address these activities. The use of false online identities or the spreading of false or misleading information about oneself or others outside of the workplace or background investigation realms, as well as the many forms of cyberbullying and malicious rumor-spreading online could be addressed. Doxing is another potentially concerning behavior that would be covered under broader language in the Personal Conduct guideline regarding disruptive, violent, or inappropriate behavior. This is

especially true of those behaviors that may not obviously be criminal in nature but could otherwise be damaging or malicious to others and raise doubts about trustworthiness, or the ability to safeguard sensitive information.

4. Handling Protected Information

As in the previous discussion of the Personal Conduct guideline, doxing is a behavior that could also be addressed in the Handling Protected Information guideline. Presently the guideline does not explicitly define what sensitive or protected information is. A government official's personal information such as home address, home phone number, or those of her children or other family members are not likely to be considered sensitive or protected. But when an individual collects and posts this information online in a manner that encourages harassment or even physical harm, that individual may be engaging in behavior that indicates poor judgment, lack of respect for the government, or an unwillingness to protect other sensitive information. This concern is elevated further if the dox contains dates of birth, social security numbers, or other non-public information, which could be considered even more sensitive in nature but not necessarily covered by this guideline. Whether they specifically include personal information as protected and thus its disclosure as potentially disqualifying, the guidelines could be more explicit in how they define what is sensitive or protected.

5. Use of Information Technology Systems

As previously identified, the Use of Information Technology Systems guideline has significant coverage of online behaviors but with one gap. Conducting vulnerability research, network reconnaissance, and visiting hacker websites were not addressed in the guideline, but may show intent to damage networks or indicate a heightened insider risk of future attacks. Should a subsequent attack actually take place, it may be difficult for a government agency to explain their failure to conduct additional background investigation or confront the applicant when this information was known beforehand. Presently, the guidelines would not provide an avenue to address this precursory behavior. The Use of Information Technology Systems guideline may need to consider

adding language that identifies this behavior as potentially disqualifying unless it can be mitigated by a plausible explanation for engaging in the activity.

6. Operations Security (New)

In light of the above discussion of lax security habits and operations security, this research proposes a new adjudicative guideline for Operations Security. The concerns cited above were that lax security habits and operations security could potentially put an individual at risk from malicious actors who could obtain their personal information more easily, and that it may also show poor judgment or a lack of basic technical abilities required to safeguard classified or sensitive information in the information age. Further discussion is recommended regarding which specific behaviors to include as disqualifying, however some of the most concerning behavior is focused in the operations security category of online activities, which includes posting public or official information on building locations, floor plans, personal identities, security procedures, pictures of key personnel or sites, or embedding geographic metadata in online postings. There may also be implications in this new guideline for addressing doxing, in that such behavior could be exposing or increasing risk to government assets or operations. Other behaviors such as downloading suspicious files or clicking unknown links in spam messages may be outside of the scope of disqualifying behavior. However, the government may need to consider what basic online personal and operations security behaviors it expects from its cleared employees, given the increasingly virtual and networked nature of national security and classified information.

7. Limitations and Avenues for Future Research

This research has attempted to identify broad trends in insider threat engagement in online activities, and compare those activities to the present personnel security adjudicative guidelines. However, there are a number of significant limitations to this study.

First the number of insider threat cases studied was extremely limited and used primarily to identify specific behaviors of insider threats. A five-year time span was used, and only cases taking place in the United States or Canada were examined. The research

would benefit from more case studies over a longer period of time and spanning more parts of the world in order to get a more complete picture of the online activities of insider threats. Second, the adjudicative case tallies taken from the DOHA website represent adjudicative appeals considered by only one group of U.S. government departments, and do not show adjudicative appeals data for other agencies or departments. Future research could seek to include more case studies, gain deeper access including subject interviews or site visits, and obtain a greater variety of adjudicative data by request from other agencies.

It is also important to note that this research made a conscious effort to avoid any sources that could potentially contain classified or sensitive information. This is especially important in understanding the activities of Bradley Manning, as much if not all of the information he allegedly disclosed to WikiLeaks has been published on the Internet. This research specifically avoided reviewing that information or any resources that may have contained that information in order to comply with information security guidelines of both DoD and DHS. It is likely, however, that such access may have provided additional insight into Manning's behaviors and activities online. Future research conducted by private or foreign entities that are not required to avoid classified or official information on the Internet may be able to gain these insights.

Another limitation of this study is that the list of online activities is based on a combination of only one other existing list and the author's own Internet research on other online behaviors. Therefore, the list of online behaviors used in this study does not represent a government-wide or discipline-wide assessment of all possible behaviors, but a best effort by the author to update and improve upon one effort. Future research could bring experts together from a variety of fields to update and validate this list in light of social and technological developments since 2009 that the author may not have found.

Recommendations on changes or modifications to the adjudicative guidelines were formulated based on the degree to which the behaviors contained in the online activities list were addressed by the guidelines. However, this list was influenced and modified as a result of the author's own online research and observations. Therefore, the evaluation of the adjudicative guidelines with respect to that list is also limited by the

research abilities and inherent biases of the author. Additionally, the author is employed in the personnel security office of a federal government agency, and has a potential bias in favor of expanding the capabilities and tools available to investigative and adjudicative entities, and less in favor of allowing applicants to expand their current levels of privacy by avoiding investigating or adjudicating their online activities.

A previously mentioned result of this research is regarding the seemingly contradictory trends of increasing online behaviors of insider threats and decreasing clearance denial cases based on misuse of information technology systems. A hypothesis to explain this was proposed, specifically, that a lack of online vetting conducted by agencies contributes to a growing blind spot in the personnel security system in which insider threats are increasing their online activities but federal agencies are not keeping up with their applicants by observing these online activities for disqualifying information. A corollary to this hypothesis is that an increase in cybervetting by background investigators will result in an increasing number of security clearance denial cases that are based on the Use of Information Technology Systems guideline. It should be noted that there may be other explanations for these apparently contradictory trends, such as the effectiveness of computer security awareness and monitoring programs, or substantive changes in the makeup of the security clearance applicant population; it is therefore all the more important that this question and hypothesis are examined in further research.

8. Conclusion

The Internet and emerging social and technological developments have enabled individuals to connect with each other in ways never before possible. Email, chat rooms, instant messaging, blogs, and social networking sites are all examples of ways to communicate and interact with the world that were not in existence in the public domain until recently. In this environment, the U.S. government must find and retain individuals for jobs in national security, including those for which a security clearance is needed. Background investigations are necessary for government agencies to evaluate the risks posed by individuals who may be more likely to cause damage or fail to protect classified information. Individuals are investigated and those investigations are adjudicated by the

employing agencies according to the personnel security adjudicative guidelines for access to classified national security information. These guidelines were issued in 1997 and most recently updated in 2005. Some of the most recent technological and social developments such as the growing popularity of social media have taken place after this time.

Given these new developments, the adjudicative guidelines may need to be re-evaluated to ensure they are keeping apace. This research used case studies and examination of security clearance appeals data to gain an understanding of the current trends in the areas of computer use and government personnel security response. The collected data, though limited in scope, appears to tentatively show that Internet activity among identified cases of insider threat is increasing, but that the number of proposed personnel security clearance denials remains steady or decreasing over the same time period. One possible explanation for this is that the present investigative techniques employed in background investigations do not search online resources where this insider threat activity may be most observable. Instead, investigators still rely on personal interviews of applicants, neighbors, friends, and coworkers to complete their investigations. Therefore, it is possible that while insider threats are increasing their online presence, the personnel security system is not doing the same, which could be leading to increasingly less relative visibility of these individuals. If this hypothesis is true, then increased use of online resources in the background investigation process could result in more, not less, security clearance denial cases due to misuse of IT systems.

The existing personnel security guidelines did not completely address the variety of new behaviors that are possible online. Specifically, improvements are recommended in the Foreign Influence, Financial Considerations, Personal Conduct, Handling Protected Information, and Use of Information Technology Systems guidelines:

- The Foreign Influence guideline could be strengthened by defining what associations or contacts are disqualifying or at least reportable.
- The Financial Considerations guideline could include language on online gaming and virtual currencies.

- The Personal Conduct guideline could expand its coverage to include all false or misleading information, not just such information when directly relevant to employment or the background investigation process.

- The Handling Protected Information guideline could more specifically identify what information is protected, and whether or not unclassified or unofficial information could be considered protected especially if it involves personal information.

- The Use of Information Technology Systems guideline could include reconnaissance activities such as port scanning or network vulnerability assessment, as well as online research of hacking, if these activities are conducted in preparation for a possible attack.

- In addition to the existing guidelines, a new guideline for Operations Security could be added, which would address behaviors that put agencies and personnel at risk such as exposing locations or details of government sites, even if those details are unclassified.

The above recommendations, along with a broad and ongoing research effort to identify emerging technologies and their implications for personnel security, may enhance the government's ability to mitigate insider risk. Consideration of these recommended changes to the personnel security adjudicative guidelines by the Office of the Director of National Intelligence could lead to a more informed and effective personnel security system. This research hopes to contribute toward that end.

APPENDIX A: PERSONNEL SECURITY ADJUDICATIVE GUIDELINES REFERENCE AID

A. INTRODUCTION:

This appendix serves as a reference aid for understanding the disqualifying conditions of the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, otherwise referred to simply as the "adjudicative guidelines." It is abbreviated from its complete form to include only the disqualifying factors, which are the most relevant to this thesis. The original paragraph markings are maintained from the complete guidelines, which accounts for why they will appear out of order here. This appendix does not substitute for the complete guidelines, which are publicly available online,[91] and its use for any purpose other than as a reference aid for this thesis is discouraged. Readers are encouraged to consult the full version for a more complete understanding of the adjudicative guidelines.

B. ALLEGIANCE TO THE UNITED STATES

4. *Conditions that could raise a security concern and may be disqualifying include:*

> (a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;
>
> (b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
>
> (c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:
>
> > (1) overthrow or influence the government of the United States or any state or local government;
> >
> > (2) prevent federal, state, or local government personnel from performing their official duties;

[91] See the Federation of American Scientists website, available at http://www.fas.org/sgp/isoo/guidelines.html.

(3) gain retribution for perceived wrongs caused by the federal, state, or local government;

(4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

C. FOREIGN INFLUENCE

7. *Conditions that could raise a security concern and may be disqualifying include:*

(a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(c) counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

(d) sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(f) failure to report, when required, association with a foreign national;

(g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

(h) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;

(i) conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

D. FOREIGN PREFERENCE

10. *Conditions that could raise a security concern and may be disqualifying include:*

(a) exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(1) possession of a current foreign passport;

(2) military service or a willingness to bear arms for a foreign country;

(3) accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;

(4) residence in a foreign country to meet citizenship requirements;

(5) using foreign citizenship to protect financial or business interests in another country;

(6) seeking or holding political office in a foreign country;

(7) voting in a foreign election;

(b) action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

E. SEXUAL BEHAVIOR

13. *Conditions that could raise a security concern and may be disqualifying include:*

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(d) sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

F. PERSONAL CONDUCT

15. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

16. *Conditions that could raise a security concern and may be disqualifying also include:*

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information

supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as

(1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

G. FINANCIAL CONSIDERATIONS

19. *Conditions that could raise a security concern and may be disqualifying include:*

(a) inability or unwillingness to satisfy debts;

(b) indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(c) a history of not meeting financial obligations;

(d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(e) consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;

(f) financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern.

(g) failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;

(h) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;

(i) compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

H. ALCOHOL CONSUMPTION

22. *Conditions that could raise a security concern and may be disqualifying include:*

(a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(e) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

(f) relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;

(g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

I. DRUG INVOLVEMENT

25. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Any drug abuse;

(b) testing positive for illegal drug use;

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(e) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(f) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) any illegal drug use after being granted a security clearance;

(h) expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

J. PSYCHOLOGICAL CONDITIONS

28. *Conditions that could raise a security concern and may be disqualifying include:*

(a) behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including

but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;

(b) an opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;

(c) the individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, e.g. failure to take prescribed medication.

K. CRIMINAL CONDUCT

31. *Conditions that could raise a security concern and may be disqualifying include:*

(a) a single serious crime or multiple lesser offenses;

(b) discharge or dismissal from the Armed Forces under dishonorable conditions;

(c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;

(d) individual is currently on parole or probation;

(e) violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

L. HANDLING PROTECTED INFORMATION

34. *Conditions that could raise a security concern and may be disqualifying include:*

(a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

(b) collecting or storing classified or other protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

(d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

(e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need to know;

(g) any failure to comply with rules for the protection of classified or other sensitive information;

(h) negligence or lax security habits that persist despite counseling by management;

(i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

M. OUTSIDE ACTIVITIES

37. *Conditions that could raise a security concern and may be disqualifying include:*

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;

(2) any foreign national, organization, or other entity;
(3) a representative of any foreign interest;

(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(b) failure to report or fully disclose an outside activity when this is required.

N. USE OF INFORMATION TECHNOLOGY SYSTEMS

40. *Conditions that could raise a security concern and may be disqualifying include:*

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

(g) negligence or lax security habits in handling information technology that persist despite counseling by management;

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

APPENDIX B: CHART OF ACTIVITIES

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Borgersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Routine and Social Uses	Social and Routine Uses of the Internet - Communications, relationship building, social interaction, or learning	Create content or postings in web forums, message boards, bulletin boards	None				1			
		Participate in social bookmarking, tagging, or folksonomies	None							
		Participate in online chat rooms	None							
		Participate in online gaming, including massively multiplayer online role playing games (MMORPGs)	None							1
		Post a comment to a web log (a.k.a. blogging)	None				1		1	1
		Use the internet for dating, finding a partner, or arranging consensual encounters with other adults	None							
		Use the internet to take online classes for college credit, personal improvement, or professional development	None							
		Send or receive online greeting cards, holiday cards, or gift cards	None							
		Send or receive emails	None	1	1		1	1	1	1
		Send messages to websites via online forms such as on "contact us" pages	None				1			
		Send or receive mass emails as part of online mailing lists or from websites of interest	None				1			
		Send or receive instant messages	None				1		1	
		Use social networking platforms	None						1	1
		Use Voice over Internet Protocol (VoIP)	None							
		Use encryption in communications	None	1				1	1	
		Use enhanced deletion or file overwrite software	None							1
		Use IP proxy or router programs such as Tor without allowing own computer to be used as a proxy by others	None							
		Use of removable storage media	None			1			1	1
		Use text messages/SMS	None							
		Use internet-based banking systems or online acquirers for credit transactions					1			
		Make online purchases of real goods	None							1
		Make online purchases of virtual goods	None							1

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Routine and Social Uses (Continued)	Unauthorized Activities in the Workplace - Online activities at work or using workplace resources that are not allowed or not authorized by the employer	Access an unauthorized website while at work or from a workplace network	16(d)(4)							
		Access gambling, shopping, auction, banking, investment management, fantasy sports, gaming, or other personal interest websites while at work or from a workplace network	16(d)(4)							
		Browse or surf websites unrelated to workplace duties	16(d)(4)							
		Build personal or non-professional websites while at work	16(d)(4)							
		Upload or download large non-professional files at work or on a workplace network, stressing workplace bandwidth	16(d)(4)							
		Download or store unauthorized personal files or software on workplace computers	16(d)(4)							
		Host web-based or local multiplayer games on workplace servers	16(d)(4)							
		Play web-based, local multiplayer, or personal games using workplace computers or networks	16(d)(4)							
		Use a company email account for personal correspondence	16(d)(4)							
		Participate in social networking platforms at work or on a workplace network.	16(d)(4)							
		Conduct business activities for self or another employer using workpace computers or networks	16(d)(4)							
		Use company servers to host personal or non-professional applications	16(d)(4)							
		Use workplace VoIP for non-professional calls	16(d)(4)							
		Stream large media files for entertainment while at work or on workplace networks, stressing bandwidth	16(d)(4)							
		Visit a website while at work that is specifically against workplace policy	16(d)(4)							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Routine and Social Uses (Continued)	Improper or Poor Information Sytems Security Habits - Behaviors that unintentionally create vulnerabilities for personal, proprietary, or sensitive government information that could be exploited or compromised	Accept or install invalid SSL certificates	None							
		Allow websites to download files to the user's computer authomatically	None							
		Allow websites to store usernames or passwords	None							
		Download files from untrusted sources	None							
		Download or install software from untrusted sources	None							
		Provide personal or financial information on untrusted, unverified, or questionable websites	None							
		Respond to website, email, or spam alerts asking for personal or financial account information	None							
		Use a non-secure or non-https connections to provide personal or financial information	None							
		Click on an untrusted, unverified, or questionable web link embedded in an e-mail	None							
		Open an e-mail or attachment from an untrusted, unverified, or questionable source	None							
		Provide personal, financial, or sensitive information to an untrusted, unverified, or questionable personal contact online	None							
		Access unsecured or non-encrypted wireless networks	None							
		Enable file sharing on a public or unsecured network	None							
		Conduct personal, financial, proprietary, or sensitive business over an open wireless router	None							
		Allow own computer to be used as a proxy or router for other users, such as being an exit point in Tor	None							
		Use a personal or public computer to improperly access a company network (such as not using a secure virtual private network (VPN)	None							
		Use weak computer, website, router, or other passwords, including passwords that are short, easy to guess, or easy to socially engineer	None							
		Use simple or easily-guessed questions and answers for password recovery or online authentication	None							
		Share passwords with others	None							
		Use the same username and password for multiple accounts	None							
		Fail to install recommended security updates or patches	None							
		Disable anti-virus, anti-malware, anti-spyware, or other essential security software	None							
		Host an unsecured FTP site	None							
		Transmit web camera (webcam) images using unsecure connections or to public, unverified, or questionable recipients.	None							
		Fail to close unused ports, leaving them open to the web	None							
		Use low or unrecommended browser security settings	None							
		Synchronize files with unsecured mobile or other devices	None							
		Unintentionally load unauthorized software or files onto a classified computer system or network	40(f)							
		Allow remote access to a personal computer system	None							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Routine and Social Uses (Continued)	Improper or Poor Practice of Operational Security (OPSEC) - Online behaviors that increase risk to the user or their agency by giving too much detail, locations, personal information	Posting information that links the user to their employer	None				1		1	
		Using official or company email addresses or usernames when posting or interacting online	None				1			
		Disclosing names or email addresses of others in public or non-private messages, such as using the "To" or "Cc" fields for a mass email when the "Bcc" field would better protect the identities of the recipients from disclosure to each other or when forwarded to others	None							
		Posting information about their employer's security measures	None						1	
		Posting information about their employer's senior management such as person details, where they live, etc.	None							
		Posting sensitive information about workplace projects, activities, etc.	None						1	
		Posting pictures of an employer's sensitive site locations or buildings	None							
		Posting pictures related to employment that contain geolocation coordinates embedded in the picture metadata	None							
		Geotagging or "checking in" at work on social media sites	None							
		Any violation of workplace OPSEC policy	None							
		Giving out a work address in online activities, including social media, online shopping, or gaming	None							
		Posting sensitive workplace information on resumes or job applications	None							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Furtherance of Illicit Activity	Explicit, Obscene, or Offensive Activities - Online behaviors that others could find morally objectionable or discomforting	Access extremist, terrorist, or other objectionable websites	None							
		Search, view, download, or purchase pornography online	None							
		Engage in remote sex, cyber-sex, or explicit online sexual dialogue with other consenting adults	None							
		Create, send, or forward spam e-mails with obscene images or text	None							
		Send or receive explicit, offensive, or violent images, movies, or other files	None							
		Use a borrowed, shared, or public computer to access pornography or other graphic websites	None							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Furtherance of Illicit Activity (Continued)	Intentional Disclosure of Classified or Sensitive Information - Online behaviors that increase the risk of unauthorized disclosure of classified or sensitive national security information (Secret, Top Secret, NATO, Restricted Data, Critical Nuclear Weapon Design Information, export-controlled, etc.	Discuss sensitive information over e-mail, instant messenger, or other online medium with foreign nationals	7(a); 7(b); 34(a); 34(g)						1	
		Discuss sensitive information over e-mail, instant messenger, or other online medium with unknown, unverified, or other questionable individuals	34(a); 34(g)							
		Download classified information onto an unclassified system	34(b); 34(c); 34(g)						1	
		Download or transmit sensitive information without permission	34(f); 34(g)						1	1
		Post sensitive information online in job applications or resumes	34(a); 34(b); 34(c); 34(g)							
		Post or transmit sensitive information to a website	34(a); 34(b); 34(c); 34(g)						1	
		Transmit sensitive information to unauthorized recipients via email, instant messenger, or other online means	34(a); 34(b); 34(c); 34(g)						1	
		Use unsecured or unaccredited instant messaging to transmit sensitive information	34(b); 34(c); 34(g)						1	

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Furtherance of Illicit Activity (Continued)	Criminal Activity - Illegal behaviors that are conducted or furthered by internet use	Obtain software licences illegally through tailored websites	16(a); 16(c)							
		Alter public or official records	16(a); 16(c)							
		Download, view, buy, sell, transmit, or store child pornography	13(a); 16(a); 16(c)							
		Download, view, buy, sell, transmit, or store copyrighted music, movies, ebooks, or other media without permission	16(a); 16(c)							
		Host a phishing platform for illegal purposes	16(a); 16(c)							
		Monitor or record online telephone conversations without permission	16(a); 16(c)							
		Use the internet to engage in money laundering including illegal transfers, structuring, layering, use of known havens, or other related activity	16(a); 16(c)							
		Use the internet to commit or facilitate credit card fraud, bank fraud, identity fraud, or other fraud	16(a); 16(c)							
		Download, buy, sell, transmit, or store unauthorized copies of software	16(a); 16(c)							
		Buy, sell, transmit, or conceal stolen items online	16(a); 16(c)							
		Solicit prostitution over the internet	16(a); 16(c)							
		Solicit underage sexual partners over the internet	13(a); 16(a); 16(c)							
		Download, view, buy, sell, transmit, or store intellectual property using the Internet	16(a); 16(c)							
		Steal proprietary information (e.g., customer records, financial records)	16(a); 16(c)							
		Create fake websites to commit fraud or theft	16(a); 16(c)							
		Use the Internet to arrange for sexual encounters with prostitutes	13(a); 16(a); 16(c)							
		Conduct blackmail or extortion over the internet	16(a); 16(c)							
		Buy, sell, or transmit illegal items such as illegal or prescription drugs, illegal or modified weapons, or explosives online	16(a); 16(c)							
		Use the internet to send money to fund or support terrorism	16(a); 16(c)				1			
		Transfering or storing funds using online gaming or other communities for the purpose of hiding or obscuring the transactions or source or destination of the money.	16(a); 16(c)							
		Engaging in illegal "Phreaking" by using computers to commit toll fraud on phones	16(a); 16(c)							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Furtherance of Illicit Activity (Continued)	Use of False or Misleading Identities - Using fake names or identities to conceal oneself and their activities	Use a fake identity when interacting with others on websites, chat rooms, or in social media	None							
		Alter message metadata to conceal the sender's identity	None							
		Use another person's identity when interacting with others on websites, chat rooms, or in social media	None							
		Falsify an online resume or job application	None							
		Conceal the sender's email address by spoofing	None							
		Falsely indicate an affiliation with an organization, company, or group online	None							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Furtherance of Illicit Activity (Continued)	Bullying, Indimidating, or Threatening Behavior - Online behaviors that individuals or groups may find embarrasing, mean, or hurtful	Disclose personal discussions of others over email or instant messenger to discredit or embarrass them	None							
		Post embarrassing, insulting, or intimidating information about a coworker or employer online	None							
		Post or share an image of someone without their permission	None							
		Post or share fictitious or damaging information about an individual or organization	None						1	
		Send an e-mail that could be hurtful or threatening to persons based on protected classes or other characteristics (age, race, religion, etc.)	None				1			
		Send threatening or intimidating messages to an organization	None							
		Sexually harass another person online	None							
		Engage in cyberbullying by using the Internet to send offensive, inappropriate verbal attacks or threats	None							
		Spread untrue or damaging information about an individual or group online	None						1	
		Use the Internet to stalk an individual or group	None							
		Doxing - posting personal information about a person with the intent of harassing, intimidating, or causing harm to the individual, or facilitating others in doing so	None							
		Swatting - using internet to report fake emergencies to authorities	31(a); (c)							
		Post intentionally misleading information about events, businesses, people, etc. for personal or political gain	None							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergerson	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Uses Specific to the Internet or Information Systems	Gaining Unauthorized Access and Bypassing Security - Attempts to obtain unauthorized access to computer systems and networks which can include bypassing established security measures	Attempt to gain other users' login and password information without authorization	34(d);							
		Conduct pre-hacking vulnerability research about computer systems or networks	None - no activity yet							
		Use password cracking software to gain unauthorized access to computer systems or networks	40(a); 40(c); 40(e); 40(f)							
		Duplicate a network router to gain unauthorized access to computer systems or networks	40(a); 40(c); 40(e); 40(f)							
		Use file transfer protocol (FTP) to gain unauthorized access to computer systems or networks	40(a); 40(c); 40(e)							
		Use hacking techniques to gain unauthorized access to a personal, business, or government computer or network	40(a); 40(c); 40(e)							
		Use hacking techniques to gain unauthorized access to a personal, business, or government user account or e-mail account	40(a)(c)(e)							
		Manipulate website URL data to obtain information from the website that is not otherwise available (hidden pages, admin rights, backup copies)	40(b)							
		Use keylogger software to obtain password information, screen shots, or other information from other computers without permission	40(a); 40(b); 40(c); 40(d); 34(d)							
		Obtain personal data through unauthorized entry into a computer database or file structure	40(a); 40(e); 34(d)						1	
		Perform pre-hacking port scanning or network reconnaissance	None - no activity yet							
		Read the email, instant messages, or chat logs of another person without their permission	40(a); 40(e)							
		Upload unauthorized software to gain access into another system	40(c); 40(f)						1	
		Use an authorized computer system to gain unauthorized access to other computer systems	40(a); 40(c)						1	
		Gain unauthorized access to a computer system or network by using an unauthorized device	40(a); 40(c); 40(e); 40(f)							
		Use administrative, unattributable, or backdoor accounts to access computer systems or networks without permission	40(a); 40(e)							
		Use spyware to collect account access information from other computers	40(a); 40(c); 40(e); 40(f); 34(d)							
		Visit hacker websites to contact hacker groups online in order to learn how to gain unauthorized access to a computer system or network	None - no activity yet							
		Access unauthorized computer systems or networks that circumvent company security measures	40(a);							
		Disable event or browser logging without authorization	40(b)							
		Disable or remove a firewall without authorization	40(b); 40(g)							
		Disable or remove anti-virus software without permission	40(b); 40(g)							
		Disable anti-virus, anti-malware, anti-spyware, or other essential security software on a workplace computer system without permission	40(b); 40(g)							
		Intentionally bypass system security measures	40(b); 40(g)							
		Lower the threshold on internet browser security settings at work	40(b); 40(g)							
		Use a proxy server to bypass restrictions, monitoring, or safeguards on company servers	40(b); 40(g)							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Uses Specific to the Internet or Information Systems (Continued)	Computer Network Sabotage - Behaviors that have the intent of injuring or attacking websites, software, or hardware of a computer system or network	Deface or make changes to a website without authorization	40(b)							
		Deploy programs that interfere with online purchasing checkout procedures	40(a); 40(b)							
		Perform a denial of service attack, which could include hosting a botnet server	40(a); 40(b)							
		Initiate a buffer overflow against a website	40(b)							
		Delete, alter, corrupt, or change operational files or systems on another computer without authorization	40(a); 40(b)							
		Intentionally run a script containing malicious code	40(b)							
		Intentionally transmit network security details to unauthorized persons or groups, such as hackers	34(a)							
		Release a virus, worm, trojan horse, or other malicious code or programs using the internet	40(b); 40(f)							
		Sabotage an online project being shared over the internet	40(a); 40(b)							
		Sabotage another computer	40(a); 40(b)							
		Set up fake user accounts on competitor websites to slow or interfere with their operations	None							
		Use malware to destroy or alter information on a computer system or network	40(a); 40(f); 40(b)							

Activity Theme	Activity Category	Example Activities	Adjudicative Guideline	Bergersen	Fondren	Nozette	Hassan	Meyers	Manning	Delisle
Total Number of Activities				2	1	1	11	2	20	9

APPENDIX C. PROPOSED OPERATIONS SECURITY GUIDELINE

A. INTRODUCTION

This thesis made a number of recommendations for updating the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information. One recommendation was the creation of a new guideline for operations security. In support of this recommendation, this appendix contains an example of what that new guideline could entail. This example is provided only as a starting point for discussion and is open to further review and development by the personnel security community.

B. GUIDELINE N: OPERATIONS SECURITY (PROPOSED)

42. *The Concern*. A failure to protect government personnel, information, information systems, equipment, and buildings from exposure to unknown, untrusted, or potentially adversarial persons, organizations, or other entities, raises doubts about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard government operations.

43. Conditions that could raise a security concern and may be disqualifying include:

> (a) deliberate or negligent disclosure of sensitive government operations information to unauthorized persons, including but not limited to personal or business contacts, the media, internet postings, or social networking platforms;
>
> (b) deliberate or negligent disclosure of personal information of federal, tribal, state, or local government personnel without permission, including but not limited to home addresses, personal phone numbers, personal email addresses, date of birth, social security number, places of worship, places of recreation, employment history, or any such information with the intent of influencing, intimidating, blackmailing, harassing, or coercing government personnel.
>
> (c) deliberate or negligent disclosure of personal information of family members or close associates of federal, tribal, state, or local government personnel without permission, with the intent of influencing, intimidating, blackmailing, harassing, or coercing government personnel.

(d) deliberate or negligent disclosure of operations security information that enables, facilitates, supports, leads to, or results in criminal activity

(e) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(f) inappropriate efforts to obtain or view sensitive government operations information outside one’s need to know

(g) negligence or lax operations security habits that persist despite counseling by management

44. Conditions that could mitigate security concerns include:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of operations security responsibilities;

(c) the operations security violations were due to improper or inadequate training;

(d) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of any affected parties;

(e) association with persons involved in such activities has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

LIST OF REFERENCES

A Complete Hacker's Handbook: Everything You Need to Know About Hacking in the Age of the Web, 1st Edition. http://www.telefonica.net/web2/vailankanni/HHB/index.html.

"Al Jazeera Interview: Anwar al Awlaki Regarding Malik Nidal Hasan," *NEFA Foundation*. December 23, 2009. Accessed July 15, 2012. http://www.nefafoundation.org/miscellaneous/NEFAal-Awlaki1209.pdf.

Brackney, Richard C., and Anderson, Robert H. *Understanding the Insider Threat: Proceedings of a March 2004 Workshop*. Santa Monica, CA: RAND Corporation, 2004. http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf.

"Bradley Manning Faces Court-martial in WikiLeaks Case." *CNN*. February 3, 2012. http://articles.cnn.com/2012-02-03/justice/justice_wikileaks-manning-court-martial_1_bradley-manning-david-coombs-julian-assange?_s=PM:JUSTICE.

Brennan, Richard J. "Canadian Spy Jeffrey Paul Delisle Pleads Guilty to Espionage Charges," *The Toronto Star*. October 10, 2012. http://www.thestar.com/news/canada/article/1268849--canadian-spy-jeffrey-paul-delisle-pleads-guilty-to-espionage-charges.

Brewster, Murray. "Harper Government had to Resist Urge to Blame Russia in Spy Case." *The Toronto Star*. May 21, 2012. http://www.thestar.com/news/canada/politics/article/1181820--harper-government-had-to-resist-urge-to-blame-russia-in-spy-case.

Carlson, Kathryn Blaze. "Decoding the Case of Alleged Canadian Spy Jeffrey Paul Delisle." *The National Post*. January 18, 2012. http://news.nationalpost.com/2012/01/18/decoding-the-case-of-alleged-canadian-spy-jeffrey-paul-delisle/.

"Chapter Nine: Phone Phreaking in the US & UK." In *A Complete Hacker's Handbook: Everything You Need to Know about Hacking in the Age of the Web*. 1st Edition. http://www.telefonica.net/web2/vailankanni/HHB/HHB_CH09.htm.

Chase, Steven, Tamara Baluja, and Jane Taber. "Accused Spy Jeffrey Delisle Led Second Life Online." *The Globe and Mail*. March 30, 2012. http://www.theglobeandmail.com/news/national/accused-spy-jeffrey-delisle-led-second-life-online/article4097146/.

Communications Security Establishment Canada. "Entrust TrueDelete Version 4.0 for Win95/NT." September 13, 2012. http://www.cse-cst.gc.ca/its-sti/services/cc/truedelete-v40-eng.html.

Cooney, Michael, "FBI Warns Emergency 911 Swatters are a Growing Menace," *Network World*, February 5, 2008. http://www.networkworld.com/community/node/24714.

Cratty, Carol, "Former State Department Official Sentenced to Life for Spying for Cuba," *CNN*, July 16, 2010. http://articles.cnn.com/2010-07-16/justice/spy.couple.sentenced_1_kendall-myers-cuban-agents-gwendolyn-steingraber-myers?_s=PM:CRIME.

"Criteria for Making Suitability Determinations." Code of Federal Regulations. Title 5, Pt. 731.202, Electronic Edition. http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=5:2.0.1.1.7&idno=5#5:2.0.1.1.7.2.1.2.

Defense Office of Hearings and Appeals. "Defense Office of Hearings and Appeals." http://www.dod.mil/dodgc/doha/ (Accessed November 18, 2012).

———. "Industrial Security Clearance Decisions." http://www.dod.mil/dodgc/doha/industrial/ (Accessed November 18, 2012).

Department of Energy. Counterintelligence Richland Field Office. "James W. Fondren, Jr." http://www.hanford.gov/c.cfm/oci/ci_spy.cfm?dossier=149 (Accessed October 29, 2012).

Department of Justice. "Defense Department Official and Two Others Arrested on Espionage Charges Involving China." February 11, 2008. http://www.justice.gov/opa/pr/2008/February/08_nsd_105.html.

———. "Former State Department Official and Wife Arrested for Serving as Illegal Agents of Cuba for Nearly 30 Years." June 5, 2009. http://www.justice.gov/opa/pr/2009/June/09-nsd-554.html.

———. "Noted Scientist Pleads Guilty to Attempted Espionage." September 7, 2011. http://www.justice.gov/opa/pr/2011/September/11-nsd-1142.html.

Dunham, Ken and Jim Melnick, *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet* (Boca Raton: Auerbach Publications, 2008).

Federal Bureau of Investigation, *Final Report of the William H. Webster Commission on The Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009*. July 12, 2012. http://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission.

Federal Bureau of Prisons. "Gregg Bergersen." *Inmate Locator.* http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=gregg&Middle=&LastName=bergersen&Race=U&Sex=U&Age=&x=0&y=0 (Accessed July 15, 2012).

———. "Gwendolyn Steingra Myers." *Inmate Locator*. http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=gwendolyn&Middle=&LastName=myers&Race=U&Sex=U&Age=&x=36&y=23 (Accessed November 14, 2012).

———. "James Fondren." *Inmate Locator*. http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=james&Middle=&LastName=fondren&Race=U&Sex=M&Age=&x=31&y=15 (Accessed July 15, 2012).

———. "Stewart Nozette." *Inmate Locator*. http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=stewart&Middle=&LastName=nozette&Race=U&Sex=U&Age=&x=0&y=0 (Accessed November 14, 2012).

———. "Tai Kuo." *Inmate Locator*. http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=tai&Middle=&LastName=kuo&Race=U&Sex=U&Age=&x=0&y=0 (Accessed July 15, 2012).

———. "Walter Kendall Myers." *Inmate Locator*. http://www.bop.gov/iloc2/InmateFinderServlet?Transaction=NameSearch&needingMoreList=false&FirstName=walter&Middle=kendall&LastName=myers&Race=U&Sex=M&Age=&x=0&y=0 (Accessed November 14, 2012).

"Forensic Analysis of Delisle's Computer." *Chronicle Herald*. October 22, 2012. http://www.scribd.com/doc/110813170/Forensic-analysis-of-Delisle-s-computer (Accessed November 14, 2012).

"4 Arrests in China Spy Cases," *Washington Times*. February 12, 2008. http://www.washingtontimes.com/news/2008/feb/12/4-arrests-in-china-spy-cases/?page=all#pagebreak.

Herbig, Katherine L. *The Evolution of Adjudicative Guidelines in the Department of Defense*. Monterey: Department of Defense Personnel Security Research Center, 2011. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA563952.

———. *Changes in Espionage by Americans, 1947-2007*. Monterey: Department of Defense Personnel Security Research Center, 2008. http://www.dhra.mil/perserec/reports/tr08-05.pdf.

Herbig, Katherine L. and Martin F. Wiskoff. *Espionage Against the United States by American Citizens, 1947-2001*. Monterrey, CA: Department of Defense Personnel Security Research Center, 2002. http://www.dhra.mil/perserec/reports/tr02-05.pdf.

Herridge, Catherine, "American Cleric Used More than 60 Email Accounts to Reach Followers, Including Hasan." *Fox News*. June 15, 2012. http://www.foxnews.com/politics/2012/06/14/al-awlaki-used-dozens-email-accounts-to-reach-followers-including-hasan/.

Hoffman, Bruce, et al.. *Insider Crime: The Threat to Nuclear Facilities and Programs*. Santa Monica: RAND Corporation, 1990. http://www.rand.org/content/dam/rand/pubs/reports/2007/R3782.pdf.

"Jeff Delisle." In *MySpace*. http://www.myspace.com/493089927 (Accessed November 6, 2012).

Jewkes, Yvonne and Majid Yar. *Handbook of Internet Crime*. Cullompton: Willan Publishing, 2010.

"Judge Cuts Sentence of Louisiana Man Who Spied for China." *Associated Press*. June 25, 2010. http://www.nola.com/crime/index.ssf/2010/06/judge_cuts_sentence_of_louisia.html.

Lemos, Robert. "Analyzing Data to Pinpoint Rogue Insiders." *Dark Reading.* November 29, 2011. http://www.darkreading.com/insider-threat/167801100/security/security-management/232200401/analyzing-data-to-pinpoint-rogue-insiders.html.

Lewis, Neil A. "Former Analyst Sentenced to Prison in Chinese Spy Case." *New York Times*. July 12, 2008. http://www.nytimes.com/2008/07/12/washington/12spy.html.

Macdonald, Alistair and Siobhan Gorman. "Canadian Military Leak to Russia Riles Allies." *Wall Street Journal*. March 28, 2012. http://online.wsj.com/article/SB10001424052702304177104577307991514394210.html.

"Milestones: Nidal Malik Hasan." *New York Times*. November 7, 2009. http://www.nytimes.com/interactive/2009/11/07/us/20091107-HASAN-TIMELINE.html.

Milewski, Terry. “5 Plot Lines in the Jeffery Delisle Navy Spy Case.” *CBC News*. October 27, 2012. http://www.cbc.ca/news/politics/story/2012/10/26/jeffrey-deslisle-spy-plotlines.html.

Nakashima, Ellen. “Bradley Manning is at the Center of the WikiLeaks Controversy. But Who is He?” *Washington Post*. May 4, 2011. http://www.washingtonpost.com/lifestyle/magazine/who-is-wikileaks-suspect-bradley-manning/2011/04/16/AFMwBmrF_story_4.html.

Office of the Director of National Intelligence. “Social Networking Study.” In Electronic Freedom Foundation. May 14, 2010. https://www.eff.org/file/31845#page/1/mode/1up.

Poulsen, Kevin and Kim Zetter. “U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe.” *Wired*. June 6, 2010. http://www.wired.com/threatlevel/2010/06/leak/.

Ragan, Steve. “The FBI’s Warning about Doxing was Too Little Too Late.” *Tech Herald*. December 19, 2011. http://www.thetechherald.com/articles/The-FBIs-warning-about-doxing-was-too-little-too-late.

“Retired AF Officer on Trial in China Spy Case.” *Associate Press*. September 22, 2009. http://www.airforcetimes.com/news/2009/09/airforce_spy_case_092209w.

Robinson, Abby. “Georgia Tech Helps to Develop a System that will Detect Insider Threats from Massive Data Sets.” Georgia Institute of Technology. November 10, 2011. http://www.gatech.edu/newsroom/release.html?nid=72599.

Rose, Andree G., et al. *Developing a Cybervetting Strategy for Law Enforcement*. Monterey, CA: International Association of Chiefs of Police and Defense Personnel Security Research Center, 2011. http://www.iacpsocialmedia.org/Portals/1/documents/CybervettingReport.pdf.

———. *Guidance for Developing a Cybervetting Strategy for National Security Positions*. Monterey, CA: Defense Personnel Security Research Center, 2011 (For Official Use Only).

Russel, Steven S., et al. *Cyber Behavior and Personnel Security: Final Report*. Minneapolis: Personnel Decisions Research Institutes, Inc., 2009.

Shaw, Eric D., Keven G. Ruby, and Jerrold M. Post. *The Insider Threat to Information Systems: The Psychology of the Dangerous Insider*. Richmond, VA: Department of Defense Security Institute, 1998. http://www.pol-psych.com/sab.pdf.

Shaw, Eric D., Lynn F. Fischer, and Andree E. Rose. *Insider Risk Evaluation and Audit*. Monterey, CA: Department of Defense Personnel Security Research Center, 2009. http://www.dhra.mil/perserec/reports/tr09-02.pdf.

Shechter, Olga, Eric Lang, and Christina Keibler. *Cyberculture and Personnel Security: Report II – Ethnographic Analysis of Second Life*. Monterey, CA: Defense Personnel Security Research Center, 2011. http://www.dhra.mil/perserec/reports/tr11-03.pdf.

U.S. Senate. Committee on Homeland Security and Governmental Affairs. *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*. February 3, 2011. http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2.

Whitlock, Craig. "Gates: Warnings of WikiLeaks Fallout Overblown." *Washington Post*. November 30, 2010. http://voices.washingtonpost.com/checkpoint-washington/2010/11/the_obama_administration_has_w.html.

Wilber, Del Quentin. " Maryland Scientist Stewart Nozette Sentenced for Passing Secrets to Supposed Mossad Agent, Expresses Regret." *Washington Post*. March 31, 2012. http://www.washingtonpost.com/blogs/crime-scene/post/maryland-scientist-stewart-nozette-sentenced-for-passing-secrets-to-mossad-expresses-regret/2012/03/21/gIQAPh52RS_blog.html.

Yost, Pete. "Cuban Spies: Kendall Myers, Gwendolyn Myers Face Prison." *Huffington Post*. July 16, 2010. http://www.huffingtonpost.com/2010/07/16/cuban-spies-kendall-myers_n_648683.html.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Robert Josefek
   Naval Postgraduate School
   Monterey, California

4. Dr. Samantha Smith-Pritchard
   Defense Personnel Security Research Center
   Monterey, California

5. Chief, Personnel Security Division
   Department of Homeland Security
   Washington, D.C.

6. Chief, Personnel Security Division
   U.S. Citizenship and Immigration Services
   Washington, D.C.